When the Sky is Falling

Network-Scale Mitigation of High-Volume Reflection/Amplification DDoS Attacks

Roland Dobbins rdobbins@arbor.net
Principal Engineer, ASERT

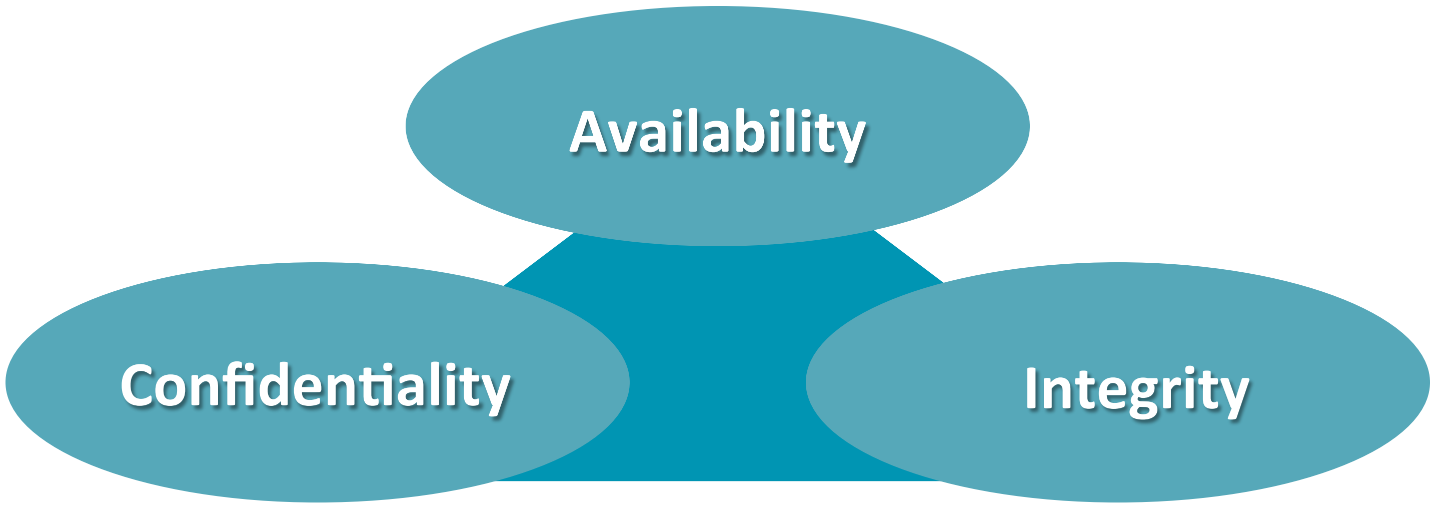
Introduction & Context

DDoS Background

What is a **D**istributed **D**enial **of** **S**ervice (DDoS) attack?

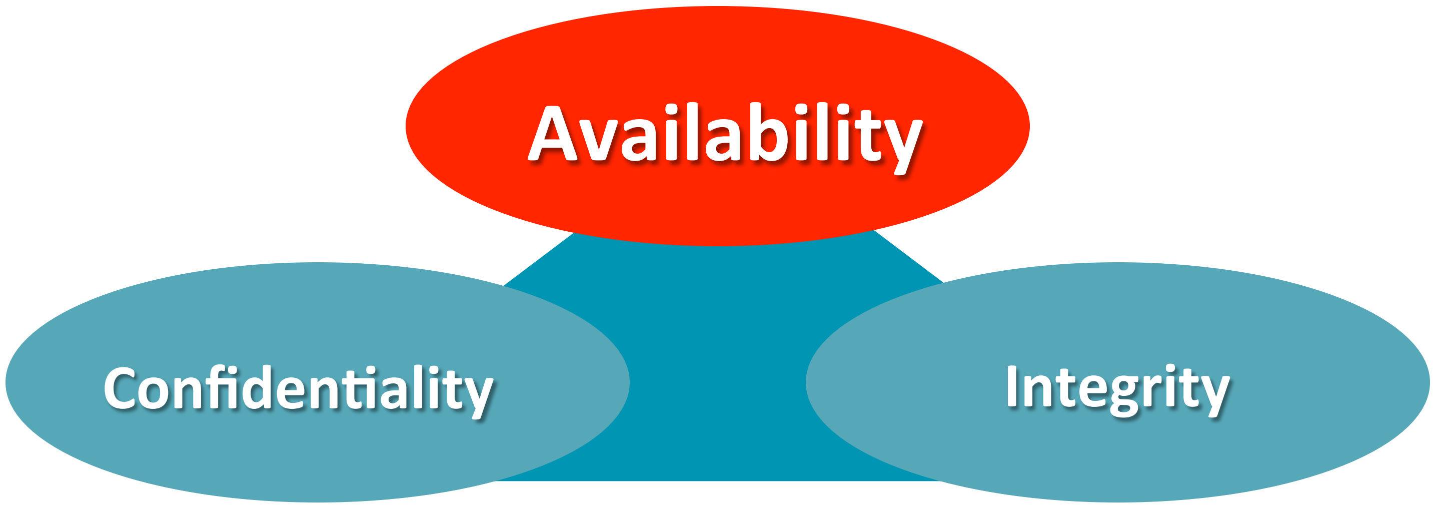
- An attempt to **consume** finite **resources**, **exploit weaknesses** in software design or implementation, or **exploit lack** of infrastructure **capacity**
- Targets the **availability** and **utility** of computing and network resources
- Attacks are almost always **distributed** for even more significant effect (i.e., DDoS)
- The **collateral damage** caused by an attack can be as bad, if not worse, than the attack itself
- **DDoS attacks affect availability**! No availability, no applications/services/data/Internet! No revenue!
- DDoS attacks are attacks **against capacity and/or state**!

Three Security Characteristics



- The goal of security is to maintain these three characteristics

Three Security Characteristics



- The primary goal of DDoS defense is maintaining availability in the face of attack

Almost All Security Spending/Effort is Focused on Confidentiality & Integrity

- Confidentiality and integrity are relatively simple concepts, easy for non-specialists to understand
- In practice, confidentiality and integrity pretty much equate to encryption - again, easy for non-specialists to understand
- The reality is that there's more to them than encryption, but it's easy to proclaim victory - "We have anti-virus, we have disk encryption, we're PCI-compliant, woo-hoo!"
- And yet, hundreds of millions of botted hosts; enterprise networks of all sizes in all verticals completely penetrated, intellectual property stolen, defense secrets leaked, et. al.
- Availability can't be finessed - the Web server/DNS server/VoIP PBX is either up or it's down. No way to obfuscate/overstate/prevaricate with regards to actual, real-world security posture.
- Availability requires operational security (opsec) practitioners who understand TCP/IP and routing/switching; who understand Web servers; who understand DNS servers; who understand security; who understand layer-7.
- These people are rare, and they don't come cheaply. Most organizations don't even understand the required skillsets and experiential scope to look for in order to identify and hire the right folks

Availability is Hard!

- Maintaining availability in the face of attack requires a combination of skills, architecture, operational agility, analytical capabilities, and mitigation capabilities which most organizations simply do not possess
- In practice, most organizations never take availability into account when designing/speccing/building/deploying/testing online apps/services/properties
- In practice, most organizations never make the logical connection between maintaining availability and business continuity
- In practice, most organizations never stress-test their apps/ services stacks in order to determine scalability/resiliency shortcomings and proceed to fix them
- In practice, most organizations do not have plans for DDoS mitigation - or if they have a plan, they never rehearse it!

Reflection/Amplification DDoS Attacks

Evolution of Reflection/Amplification DDoS Attacks

- Many varieties of reflection/amplification DDoS attacks have been observed ‘in the wild’ for **18 years or more.**
- Beginning in October of 2013, high-profile NTP reflection/ amplification DDoS attacks were launched against various **online gaming** services.
- With **tens of millions of simultaneous users** affected, these attacks were reported in the mainstream tech press.
- But these attacks aren’t new – the **largest observed DDoS attacks** are all reflection/amplification attacks, and **have been for years**.
- Reflection/amplification attacks require the ability to **spoof the IP address** of the intended target.
- In most volumetric DDoS attacks, throughput (pps) is more important that bandwidth (bps). In most reflection/amplification DDoS attacks, **bps is more important than pps** – it fills the pipes!

Components of a Reflection/Amplification DDoS Attack

Amplification

- Attacker makes a relatively small request that generates a significantly-larger response/reply. This is true of most (not all) server responses.

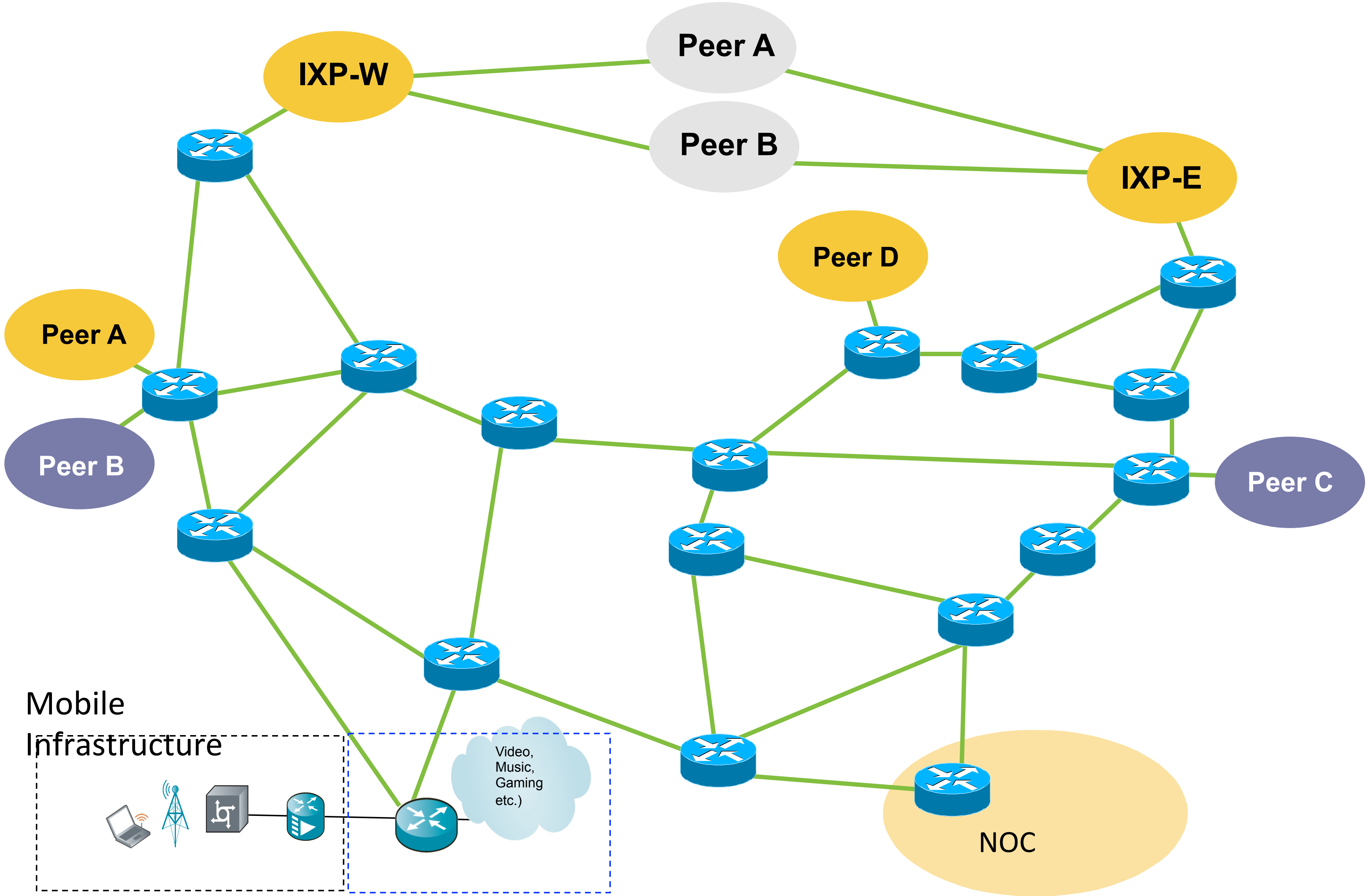
Reflection

- Attacker sends spoofed requests to a large number of Internet connected devices, which reply to the requests. Using IP address spoofing, the ‘source’ address is set to the actual target of the attack, where all replies are sent. Many services can be exploited to act as reflectors.

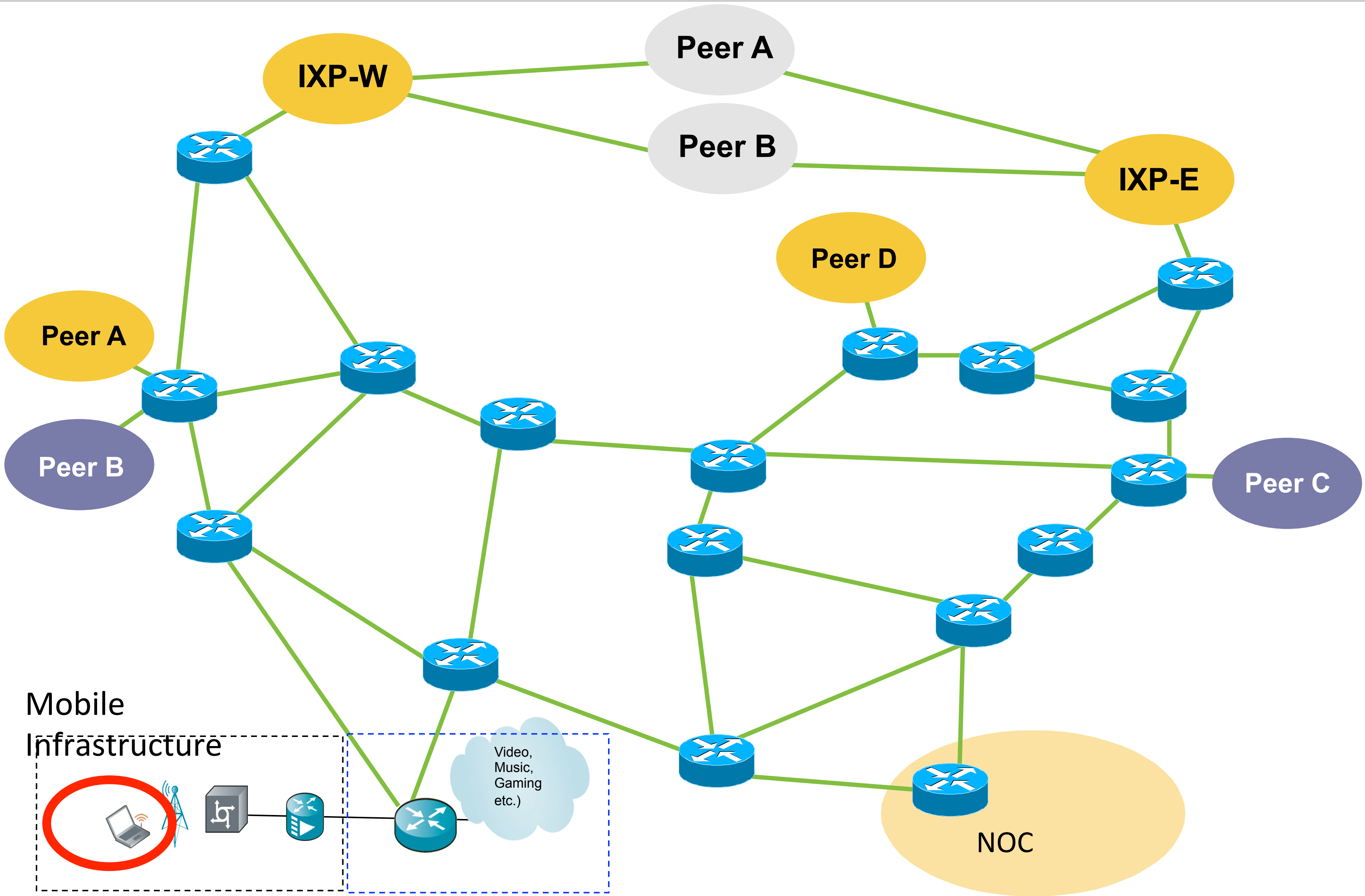
Impact of Reflection/Amplification DDoS Attacks

- Servers, services, applications, Internet access, et. al. on the target network ***overwhelmed and rendered unavailable*** by sheer traffic volume – tens or hundreds of gb/sec frequent.
- ***Complete saturation*** of peering links/transit links of the target network.
- ***Total or near-total saturation*** of peering links/transit links/core links of intermediate networks between the reflectors/amplifiers and the target network – including the networks of direct peers/ transit providers of the target network
- ***Widespread collateral damage*** – packet loss, delays, high latency for Internet traffic of uninvolved parties which simply happens to traverse networks saturated by these attacks.
- ***Unavailability*** of servers/services/applications, Internet access for bystanders topologically proximate to the target network.

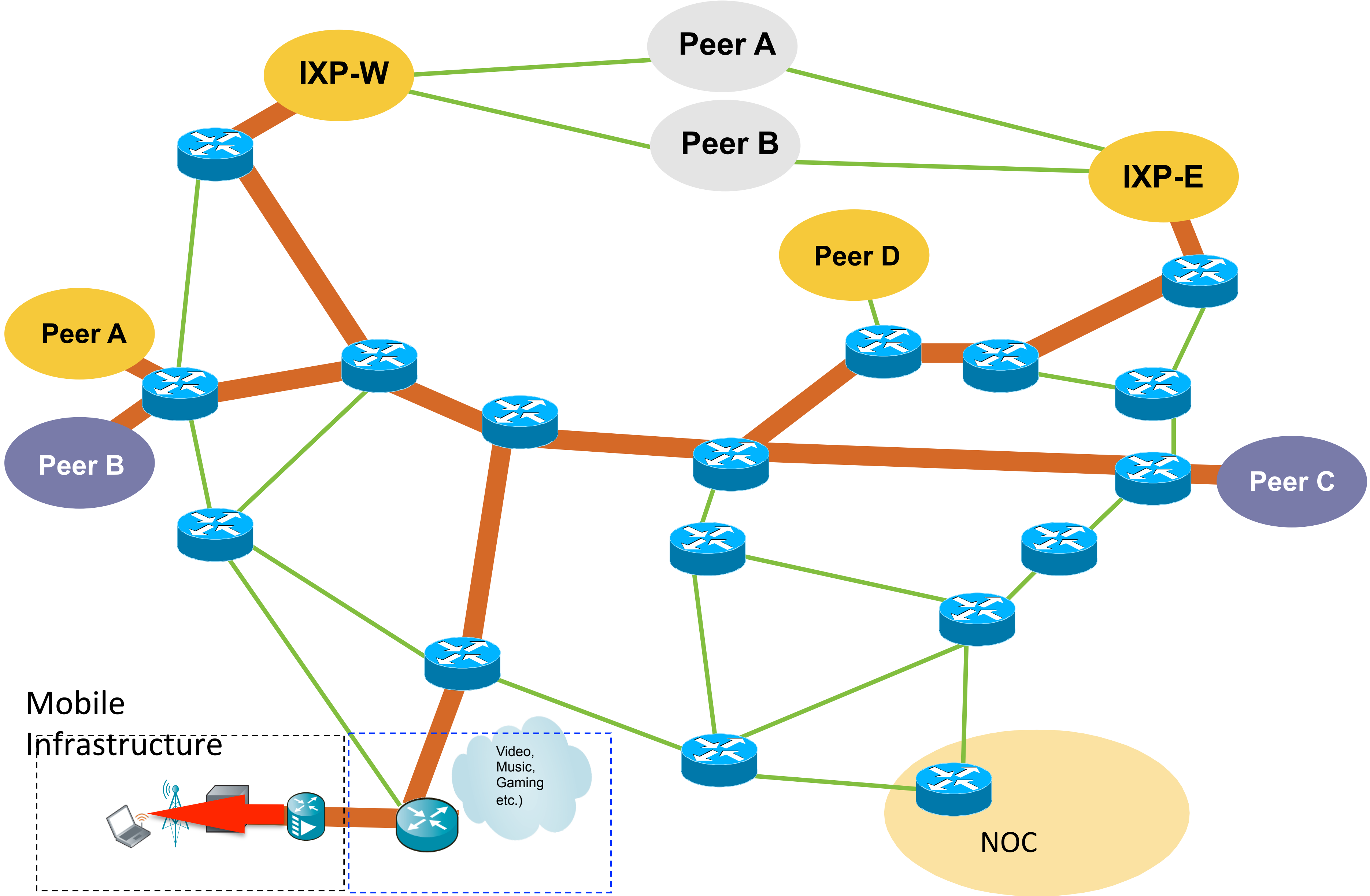
Effects of a 400gb/sec Reflection/Amplification DDoS Attack on Network Capacity



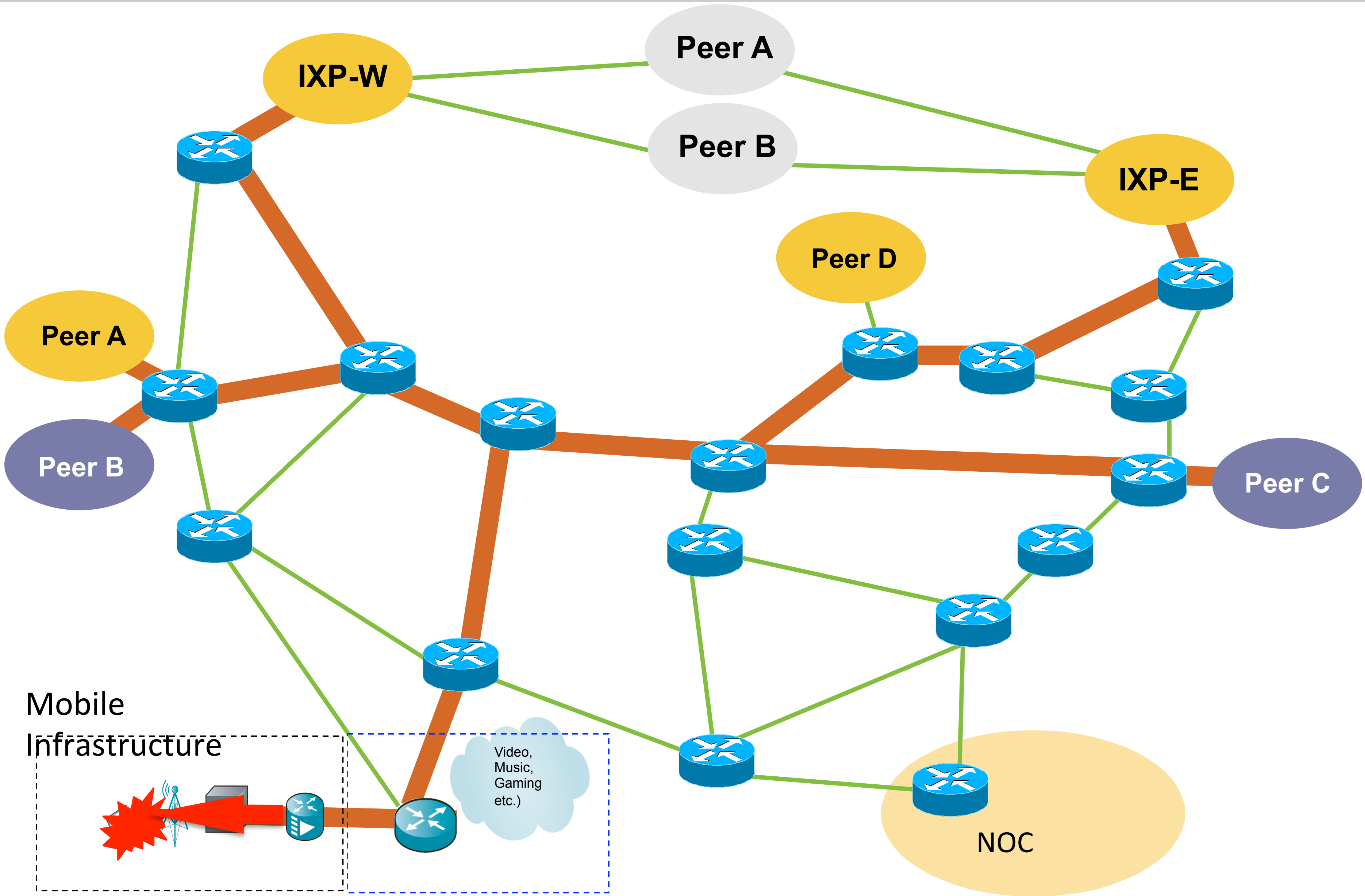
Effects of a 400gb/sec Reflection/Amplification DDoS Attack on Network Capacity



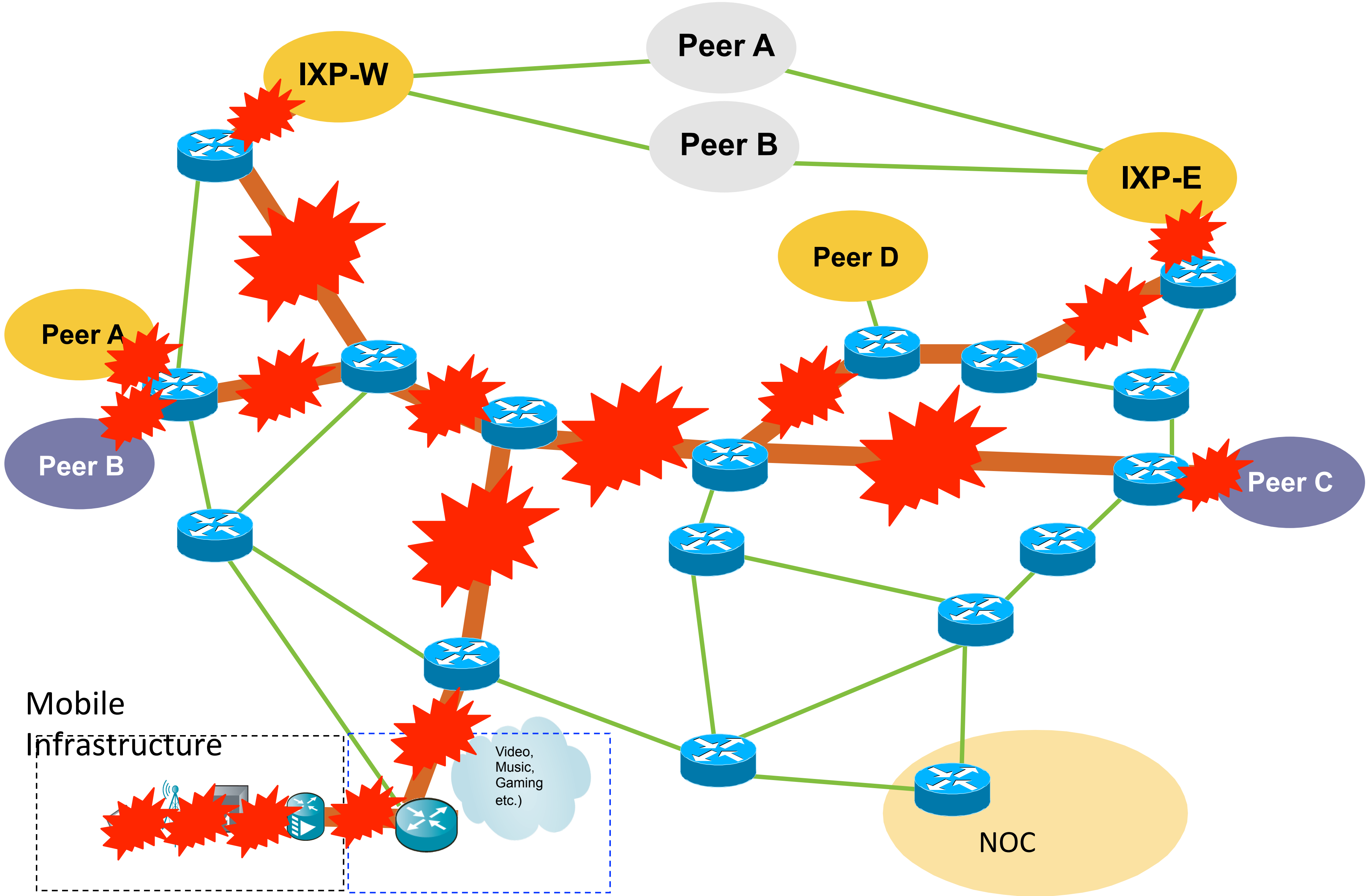
Effects of a 400gb/sec Reflection/Amplification DDoS Attack on Network Capacity



Effects of a 400gb/sec Reflection/Amplification DDoS Attack on Network Capacity



Effects of a 400gb/sec Reflection/Amplification DDoS Attack on Network Capacity



The Two Main Factors Which Make These Attacks Possible

- Failure to deploy ***source-address validation (e.g., anti-spoofing) mechanisms*** such as Unicast Reverse-Path Forwarding (uRPF), ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, ACLs, etc. on ***all*** edges of ISP and enterprise networks.

- ***Misconfigured, abusable services*** running on servers, routers, switches, home CPE devices, etc.

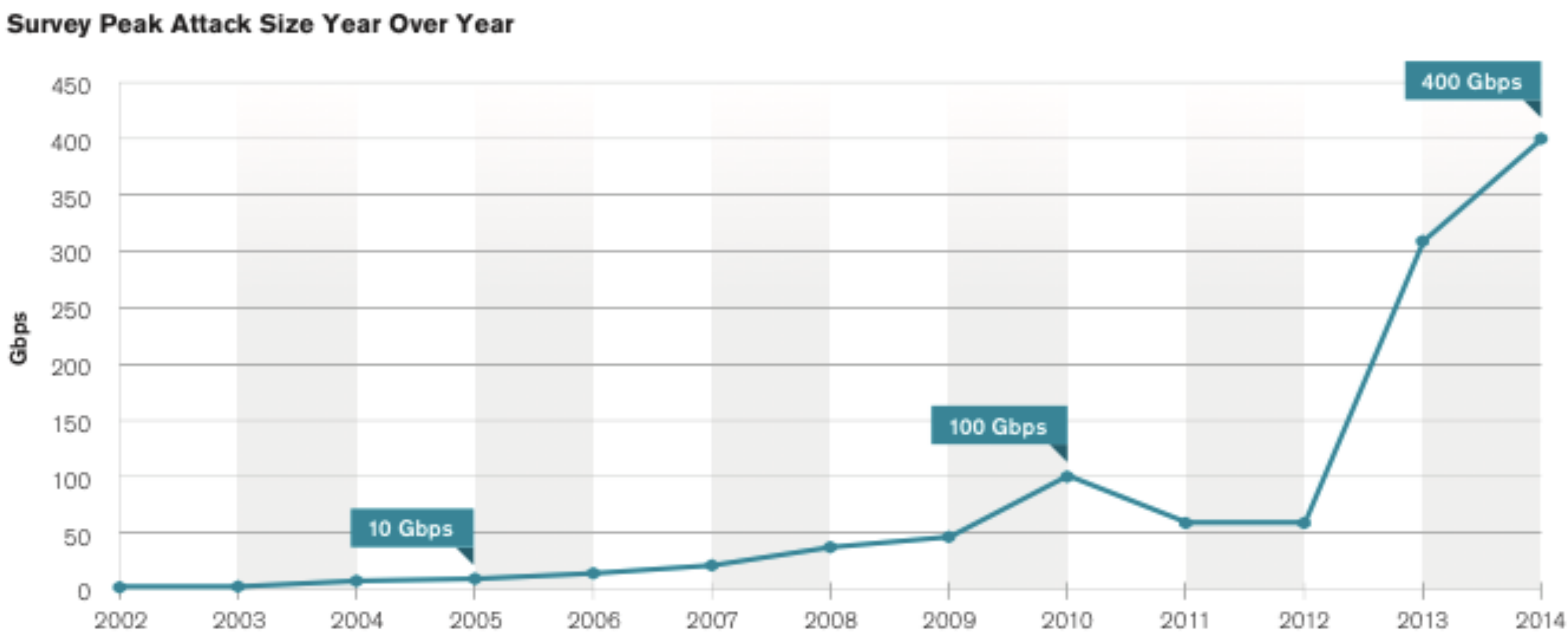
The Two Main Factors Which Make These Attacks Possible

- Failure to deploy ***source-address validation (e.g., anti-spoofing) mechanisms*** such as Unicast Reverse-Path Forwarding (uRPF), ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, ACLs, etc. on ***all*** edges of ISP and enterprise networks.

- ***Misconfigured, abusable services*** running on servers, routers, switches, home CPE devices, etc.

Growth of DDoS Attack Volumes, 2002 - 2014

Virtually *all* growth in DDoS attack volume over the last 12 years is due to the rise in popularity of reflection/amplification DDoS attack methodologies.



The ability to spoof traffic is *required* in order to launch reflection/amplification DDoS attacks.

Additional Contributing Factors

- Failure of network operators to utilize ***flow telemetry*** (e.g., NetFlow, cflowd/jflow, et. al.) collection and analysis for attack detection/classification/traceback.
- Failure of ISPs and enterprises to ***proactively scan for and remediate abusable services*** *on their networks* and to scan for and alert customers/users running abusable services – ***blocking abusable services*** until they are remediated, if necessary.
- Failure to deploy and effectively utilize ***DDoS reaction/mitigation tools*** such as Source-Based Remotely-Triggered Blackholing (**S/RTBH**), **flowspec**, and Intelligent DDoS Mitigation Systems (**IDMS**es).
- Failure to ***fund and prioritize availability*** equally with confidentiality and integrity in the security sphere.
- ***Failure*** of many enterprises/ASPs to subscribe to *'**Clean Pipes**'* DDoS mitigation services offered by ISPs/MSSPs.

What Types of Devices Are Being Abused?

- ***Consumer broadband customer premise equipment (CPE)*** devices – e.g., home broadband routers/modems with insecure (and sometimes insecurable!) factor default settings
- ***Commercial-grade provider equipment (PE) devices*** – e.g., larger, ***more powerful routers and layer-3 switches*** used by ISPs and enterprises
- ***Servers (real or virtual)*** running misconfigured, abusable service daemons – home servers set up by end-users, commercial servers set up by ISPs and enterprises.
- ***Embedded devices*** like network-connected printers (!), DVRs, et. al.
- The ***Internet of Things*** is rapidly becoming the ***Botnet of Things***!

Reflection/Amplification Attack Terminology

- ***Attack source*** – origination point of spoofed attack packets.
- ***Reflector*** – nodes through which spoofed attack packets are 'reflected' to the attack target and/or to a separate amplifier node prior to reflection to the target.
- ***Amplifier*** – nodes which receives non-spoofed attack packets from reflector nodes and then generate significantly larger response packets, which are sent back to the reflectors.
- ***Reflector/Amplifier*** – nodes which performs both the reflection and amplification of attack packets, and then transmit the non-spoofed, amplified responses to the ultimate target of the attack. Many (not all) reflection/amplification attacks work this way.
- ***Attack leg*** – the distinct logical path elements which attack traffic traverses on the way from the attack source to reflectors/ amplifiers, and from reflectors/amplifiers to the attack target.

Spoofed vs. Non-spoofed Traffic

- Attack source – reflector/amplifier source IP addresses are ***spoofed***. The attacker ***spoofs*** the IP address of the ultimate target of the attack.
- If separate reflectors and amplifiers are involved, the traffic from the reflector to the amplifier is ***not spoofed***, the traffic from the amplifier back to the reflector is ***not spoofed***, and the traffic from the reflector to the attack target is ***not spoofed***.
- If combined reflectors/amplifiers are involved, the traffic from the reflectors/amplifiers to the attack target is ***not spoofed***.
- This means that the attack target sees the ***real IP addresses*** of the attack traffic pummeling it on the ultimate leg of the attack.
- This fact has significant ***positive implications for the mitigation options*** available to the attack target – but ***the sheer number of source IPs*** is often a complicating factor.

Five Common Reflection/Amplification Vectors

- **chargen** – 30-year-old tool for testing network link integrity and performance. Seldom (ever?) used these days for its original intended purpose. Senselessly, absurdly implemented in the modern age by clueless embedded device vendors.
- **DNS** – the Domain Name System resolves human-friendly names into IP addresses. Part of the ‘control-plane’ of the Internet. No DNS = no Internet.
- **SNMP** – Simple Network Management Protocol. Used to monitor and optionally configure network infrastructure devices, services, etc.
- **NTP** – Network Time Protocol provides timesync services for your routers/switches/laptops/tablets/phones/etc. The most important Internet service you’ve never heard of.
- **SSDP** – Simple Services Discovery Protocol acts as a poorly designed-and-implemented services enumeration system for the poorly-designed-and-implemented UPnP.

Reflection/Amplification Isn't Limited to These Five Vectors

- Many protocols/services can be leveraged by attackers to launch reflection/amplification DDoS attacks.
- These five– DNS, chargen, SNMP, SSDP, and NTP – are commonly-observed reflection/amplification vectors.
- Most (not all) reflection/amplification attacks utilize UDP.
- The same general principles discussed with regards to these five vectors apply to others, as well.
- There are protocol-/service-specific differences which also apply.
- Attackers are investigating and actively utilizing other reflection/amplification vectors, as well – be prepared!

Five Common Reflection/Amplification Vectors

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

NTP Reflection/Amplification

Amplification Factor - NTP

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

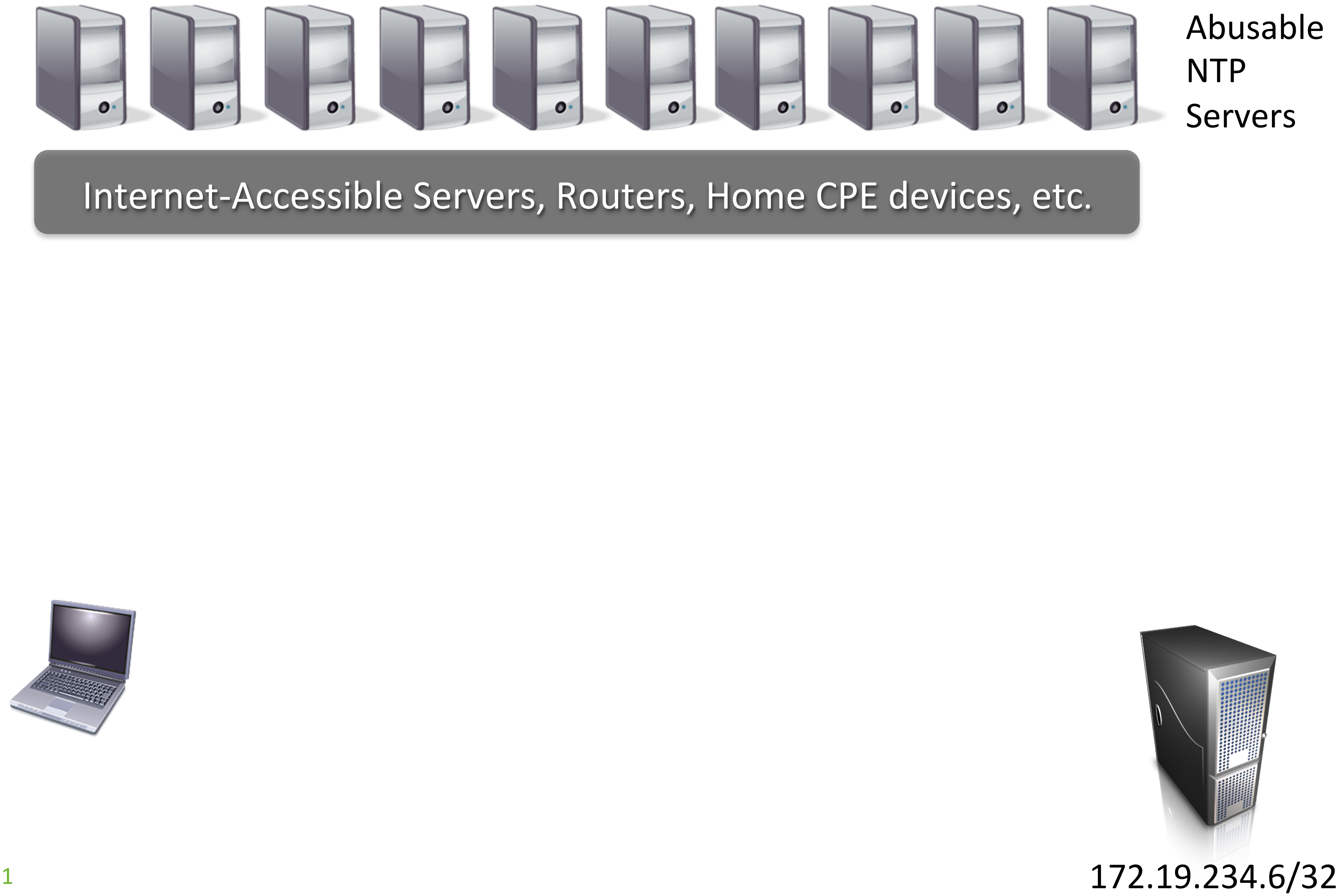
Characteristics of an NTP Reflection/Amplification Attack

- The attacker ***spoofs*** the IP address of the target of the attack, sends *monlist*, *showpeers*, or other NTP level-6/-7 administrative queries to multiple abusable NTP services running on servers, routers, home CPE devices, etc.
- The attacker chooses the UDP port which he'd like to target – typically, UDP/80 or UDP/123, but it can be ***any port of the attacker's choice*** – and uses that as the source port. The ***destination port is UDP/123***.
- The NTP services 'reply' to the attack target with ***non-spoofed*** streams of ~468-byte packets ***sourced from UDP/123*** to the target***; the destination port is the source port the attacker chose*** when generating the NTP *monlist*/*showpeers*/etc. queries.

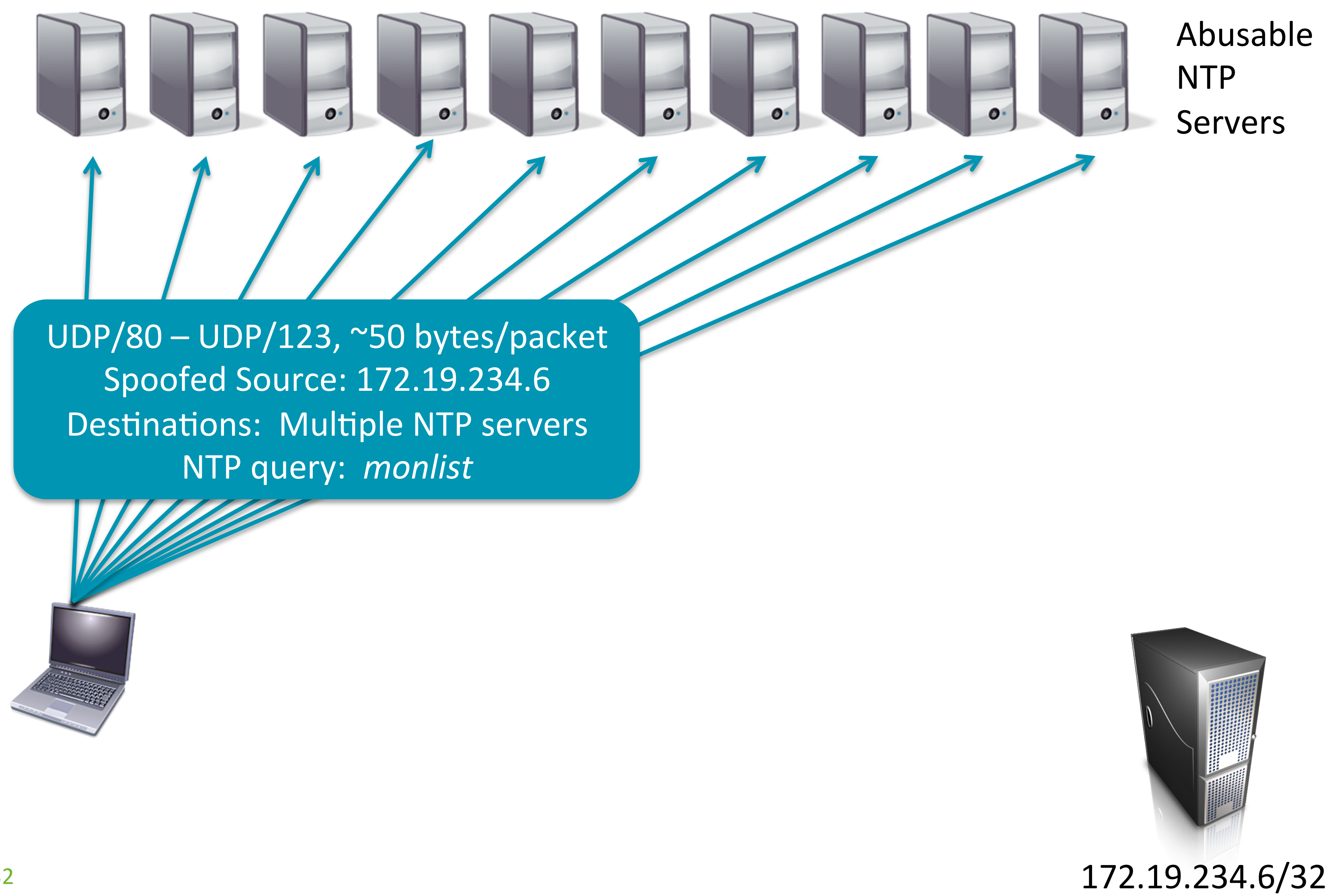
Characteristics of an NTP Reflection/Amplification Attack (cont.)

- As these multiple streams of ***non-spoofed*** NTP replies converge, the attack volume can be ***huge*** – the largest verified attack of this type so far is ***over 300gb/sec***. ***100gb/sec*** attacks are commonplace.
- Due to sheer attack volume, the ***Internet transit bandwidth*** of the target, along with core bandwidth of the target's peers/upstreams, as well as the core bandwidth of intermediary networks between the various NTP services being abused and the target, is ***saturated*** with ***non-spoofed*** attack traffic.
- In most attacks, between ~4,000 - ~7,000 abusable NTP services are leveraged by attackers. ***Up to 50,000 NTP services*** have been observed in some attacks.

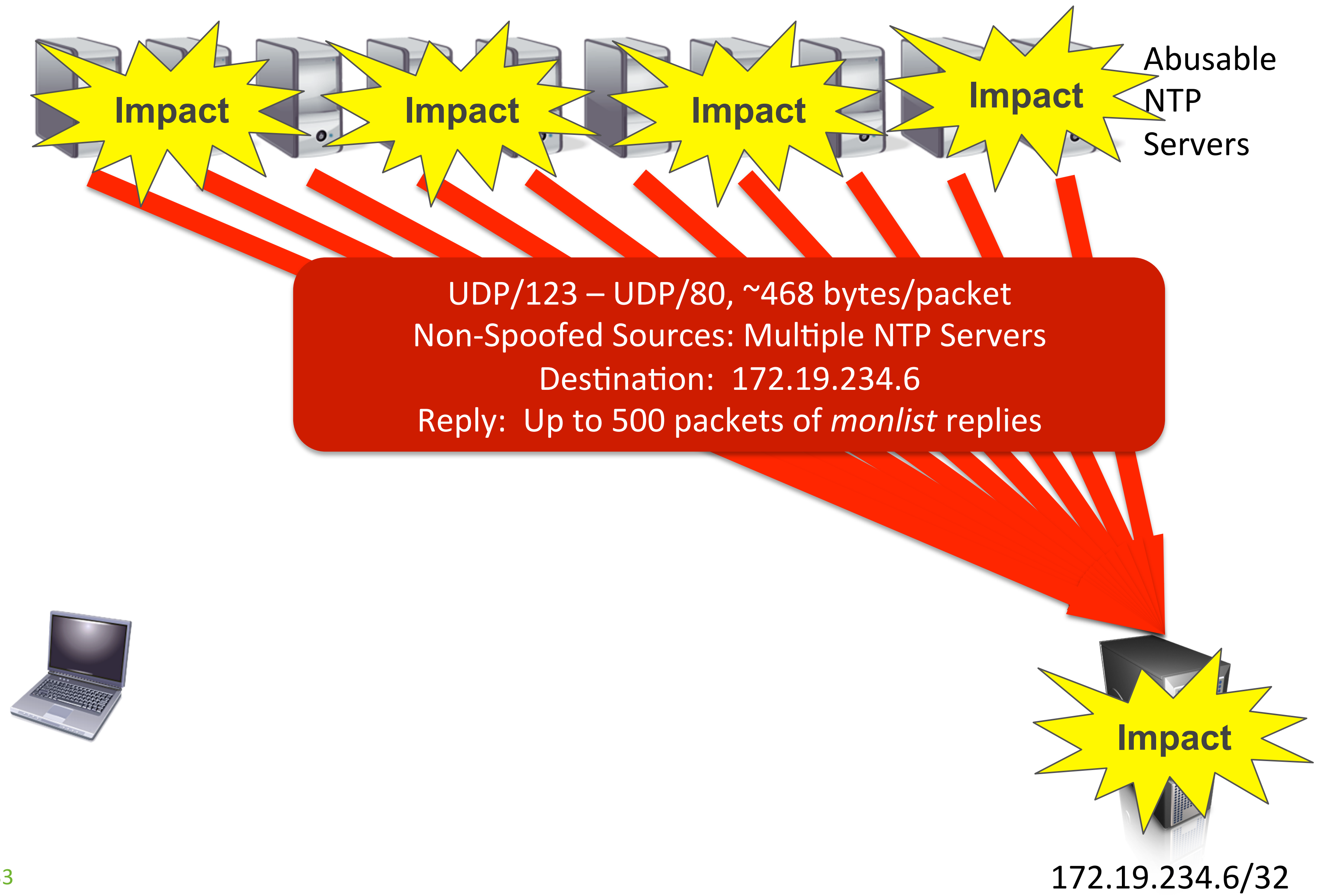
NTP Reflection/Amplification Attack Methodology



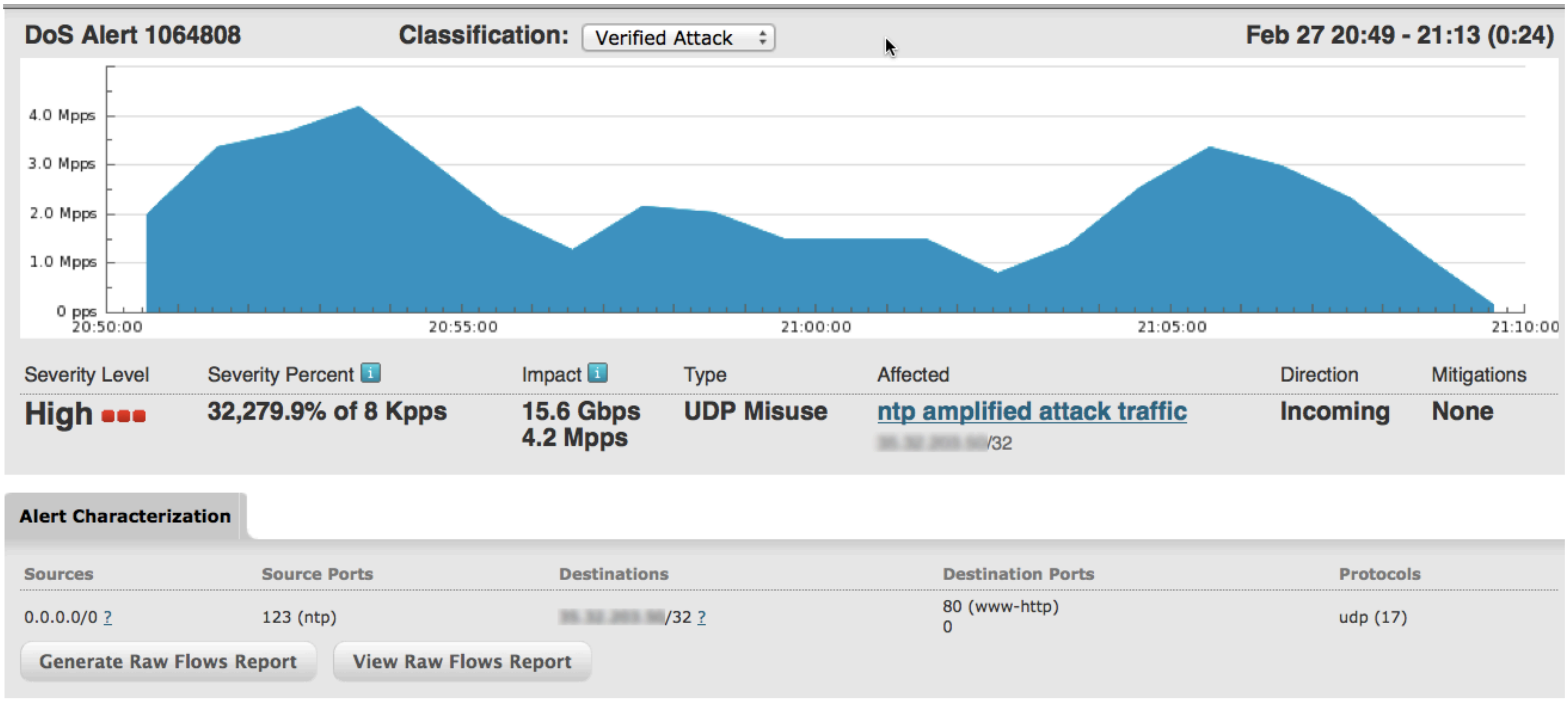
NTP Reflection/Amplification Attack Methodology



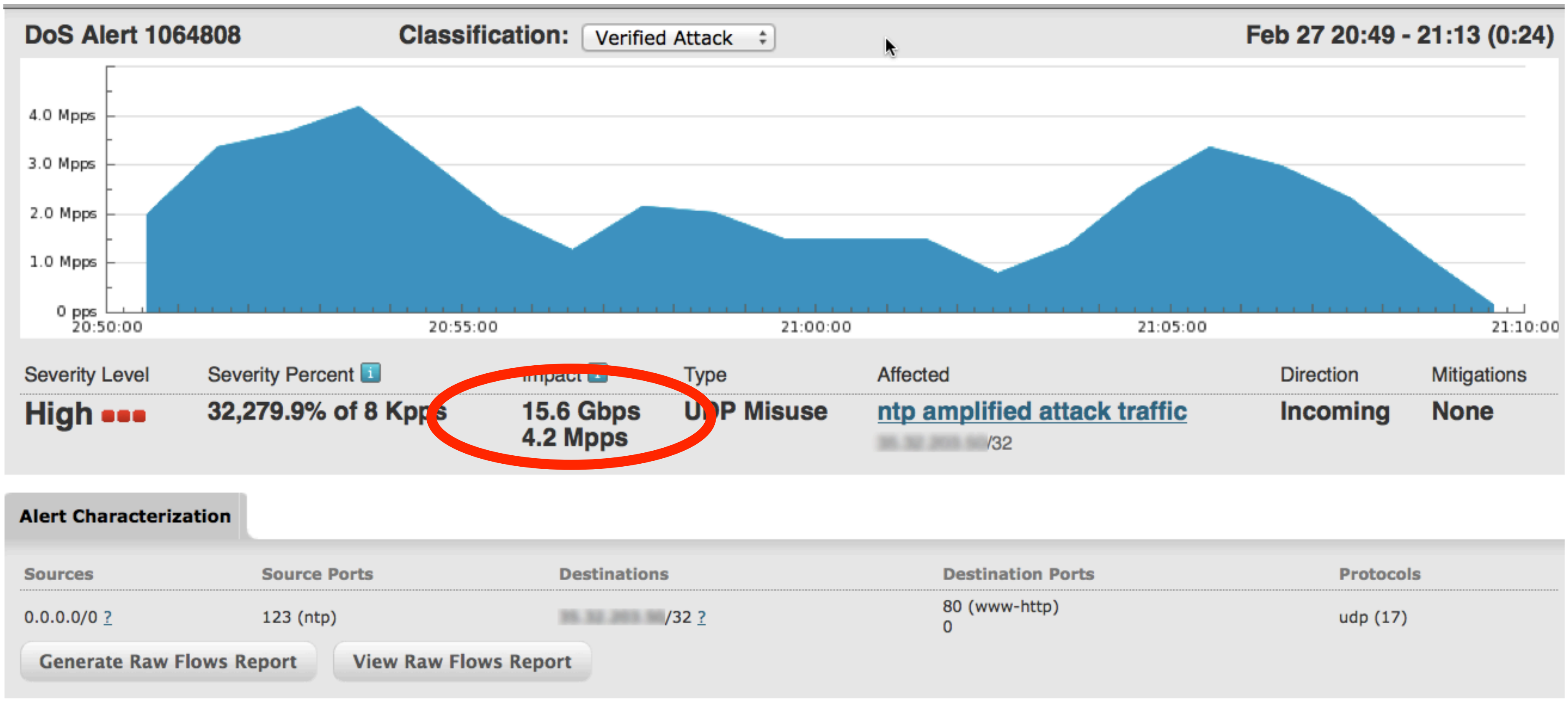
NTP Reflection/Amplification Attack Methodology



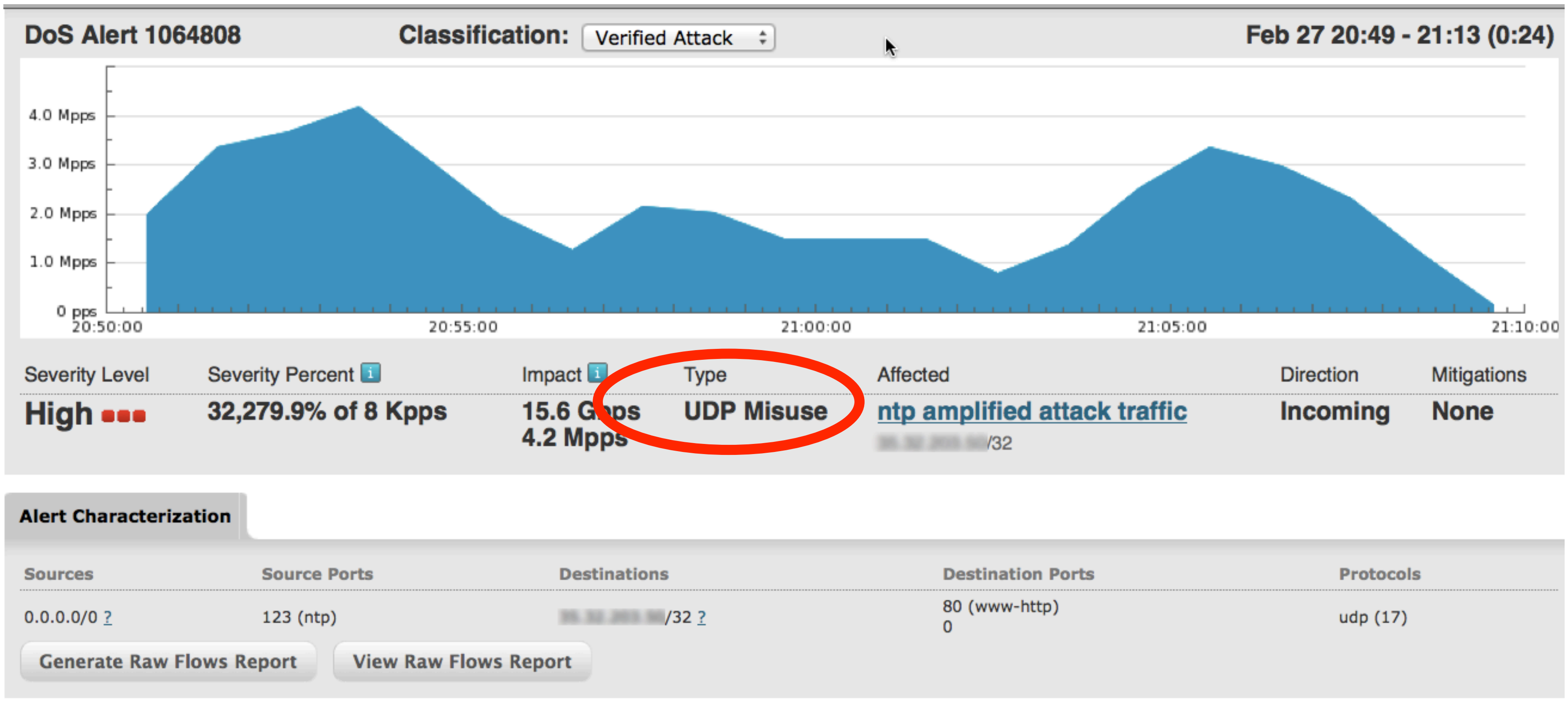
NTP Reflection/Amplification Attack



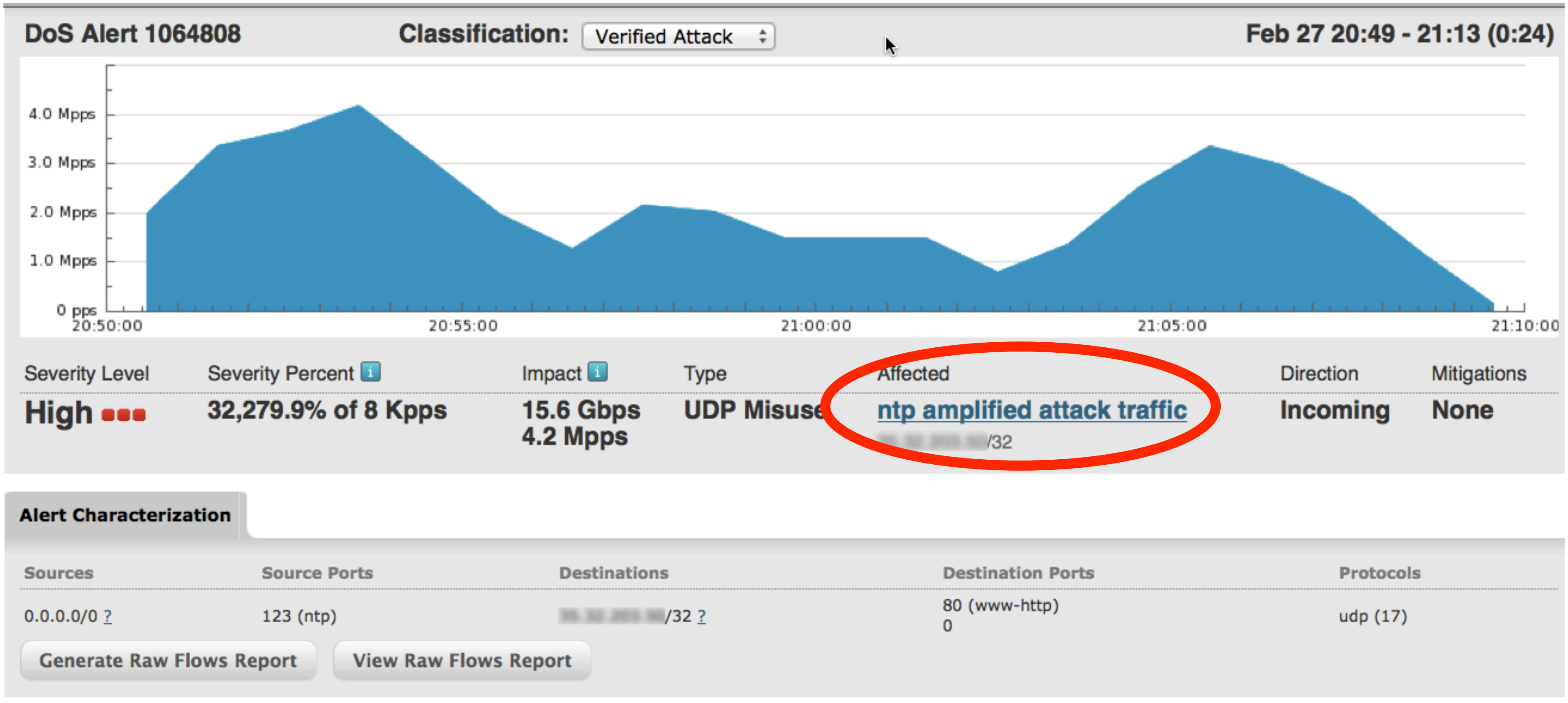
NTP Reflection/Amplification Attack



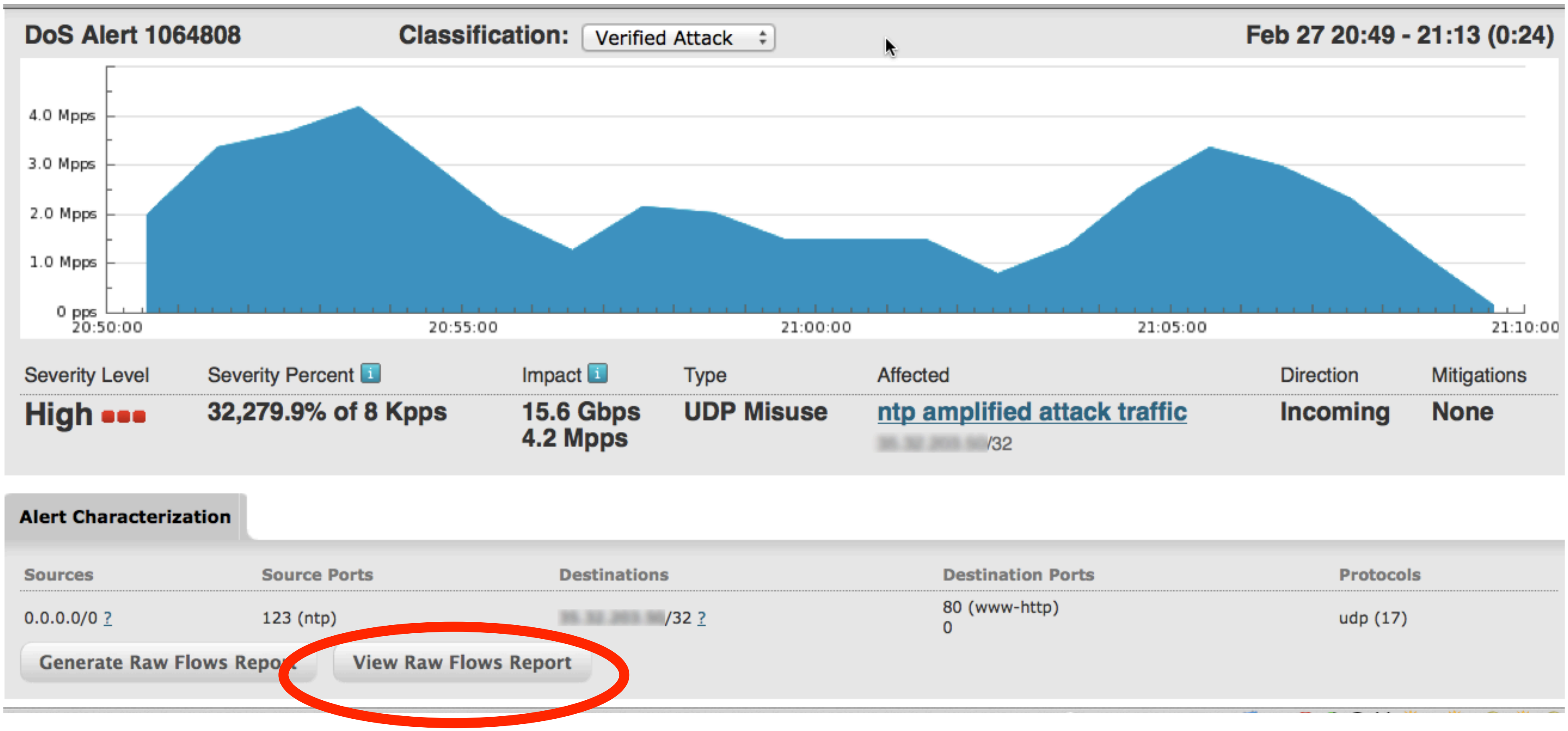
NTP Reflection/Amplification Attack



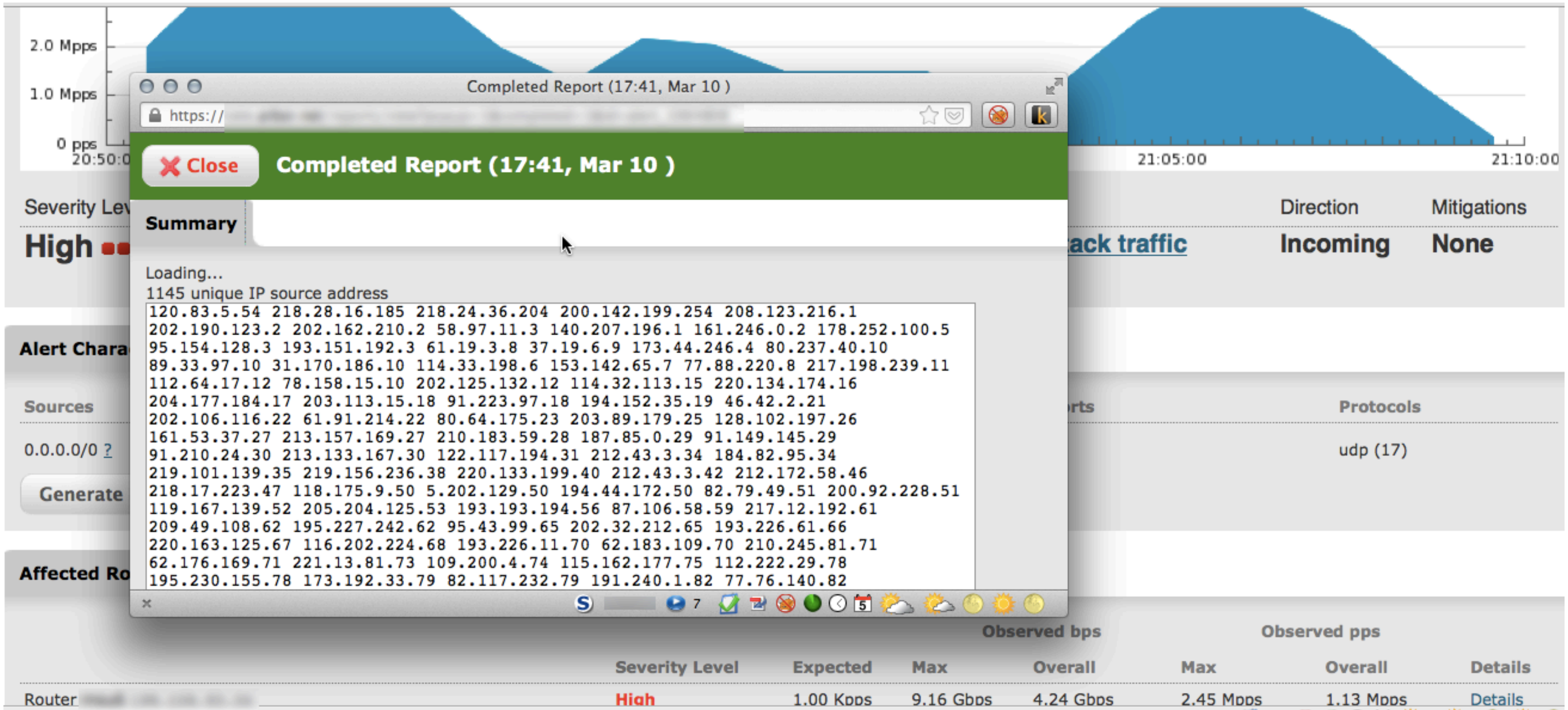
NTP Reflection/Amplification Attack



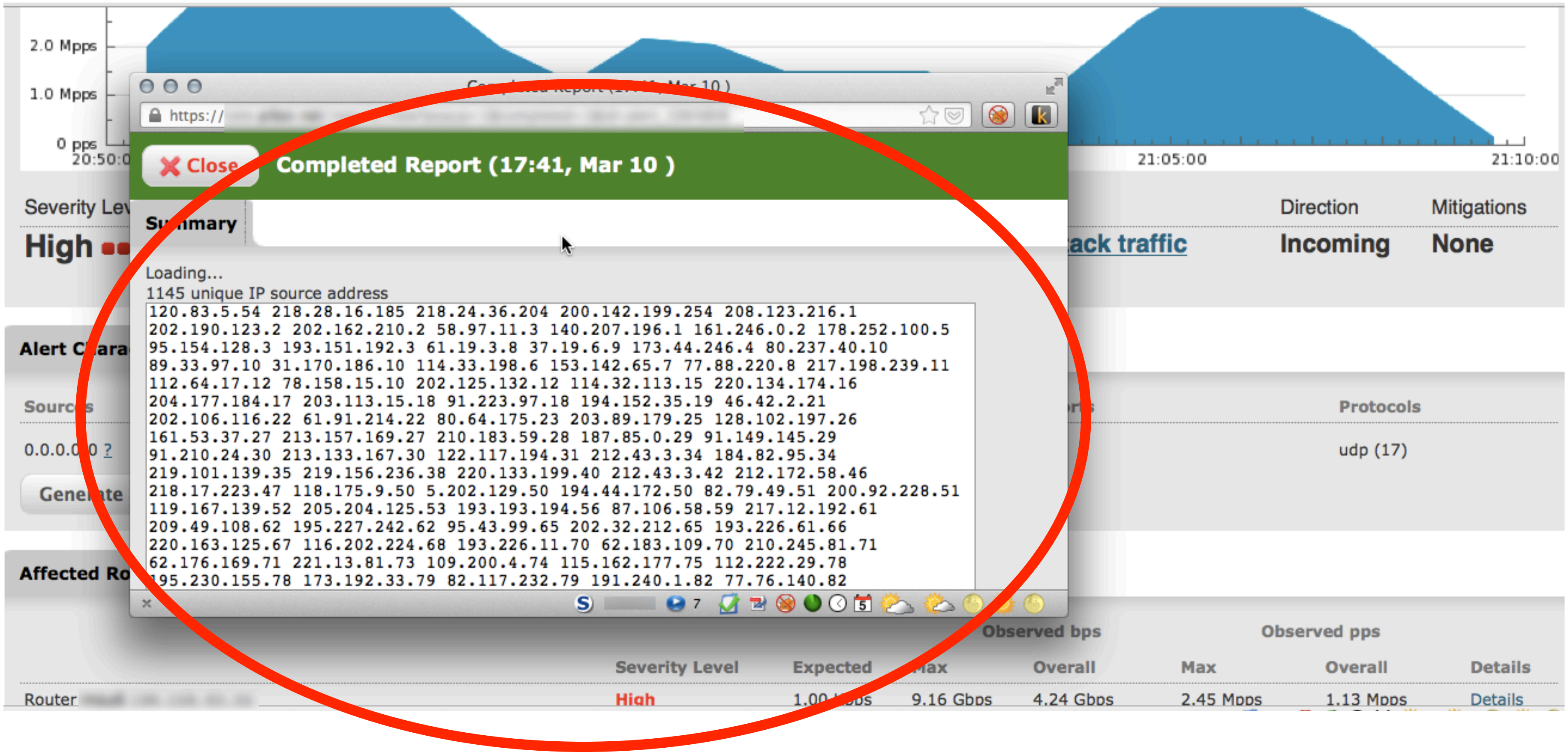
NTP Reflection/Amplification Attack



NTP Reflection/Amplification Attack



NTP Reflection/Amplification Attack



NTP Reflection/Amplification Attack

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router [illegible]	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 [illegible]		-	9.16 Gbps	4.24 Gbps	2.45 Mpps	1.13 Mpps	Details
Router [illegible]	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 [illegible]		-	2.50 Mbps	2.40 Mbps	666.00 pps	641.67 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [illegible]		-	2.23 Gbps	1.05 Gbps	594.90 Kpps	280.40 Kpps	Details
Interface (SNMP 521) xe-5/1/0.106 [illegible]		-	1.13 Gbps	693.04 Mbps	301.08 Kpps	185.48 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [illegible]		-	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!

NTP Reflection/Amplification Attack

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!

NTP Reflection/Amplification Attack

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

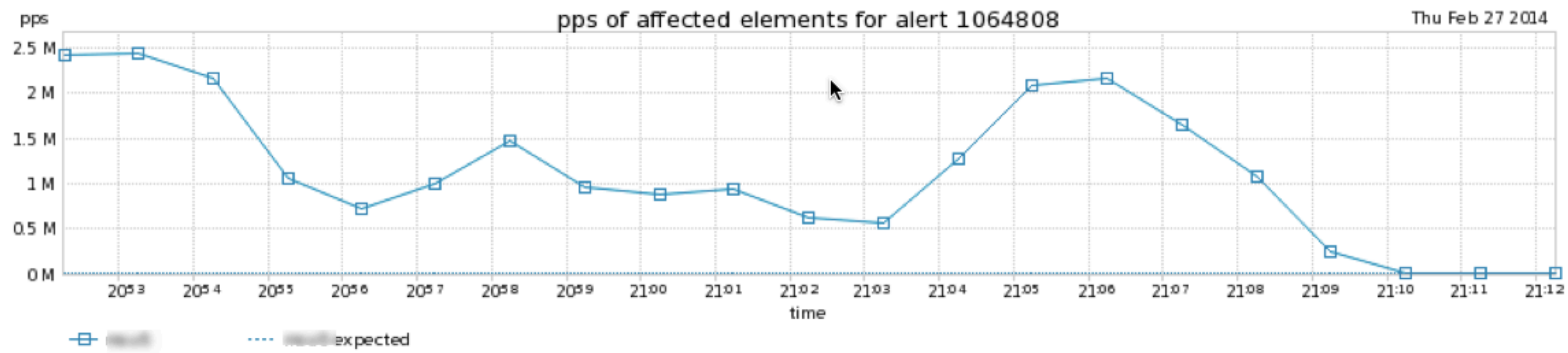
Escalated

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

NTP Reflection/Amplification Attack

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 /32 ntp amplified attack traffic



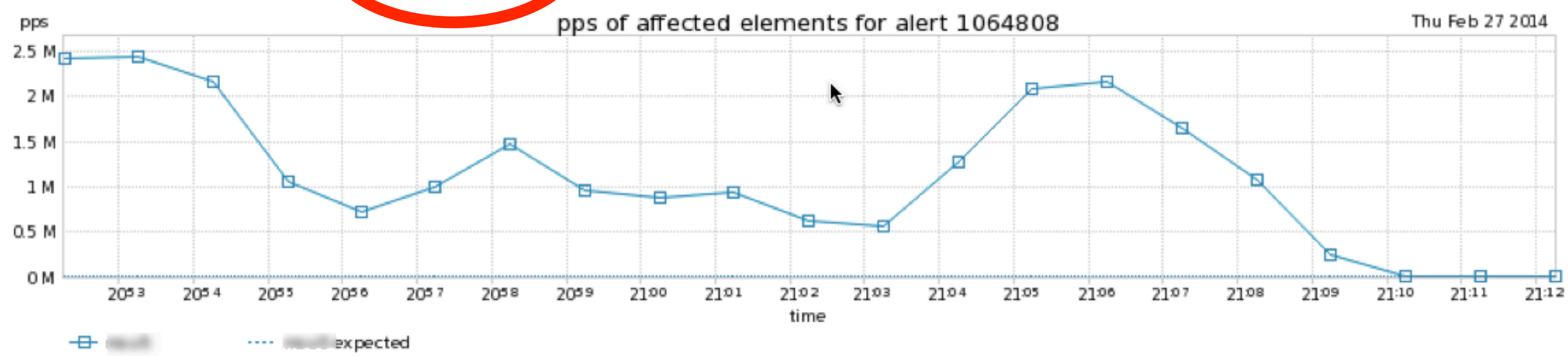
Affected Network Elements

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

NTP Reflection/Amplification Attack

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 /32 ntp amplified attack traffic



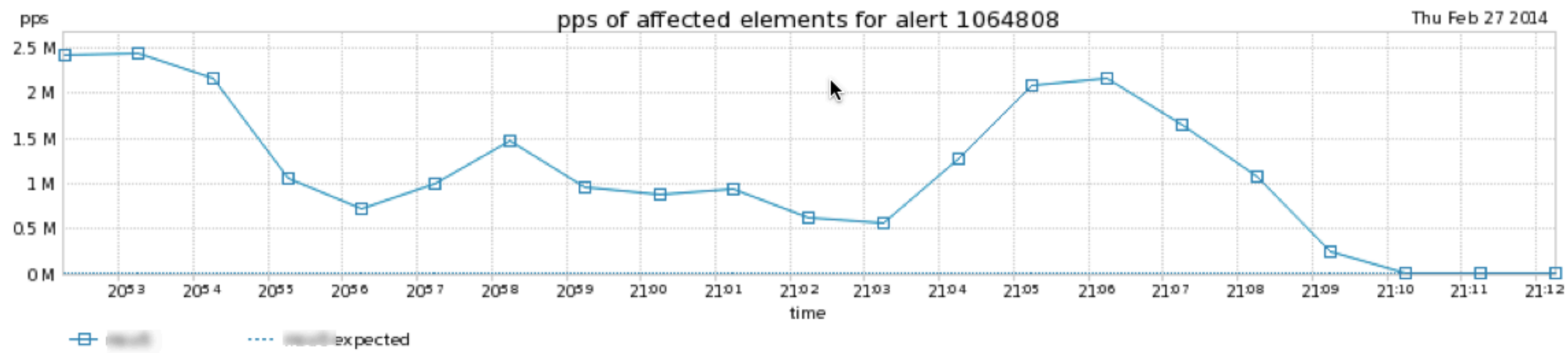
Affected Network Elements

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

NTP Reflection/Amplification Attack

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 [illegible]/32 ntp amplified attack traffic



Affected Network Elements

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

NTP Reflection/Amplification Attack

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

NTP Reflection/Amplification Attack

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

NTP Reflection/Amplification Attack

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[illegible]/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

NTP Reflection/Amplification Attack

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[illegible]/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

NTP Reflection/Amplification Attack

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 [illegible]	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 [illegible]	124	522.34 G	1.12 G	467.77	3.32 G	886.95 k	78.26	☑
xe-0/0/0.20 [illegible]	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

NTP Reflection/Amplification Attack

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

NTP Reflection/Amplification Attack

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

DNS Reflection/Amplification

Amplification Factor - DNS

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

Characteristics of a DNS Reflection/Amplification Attack

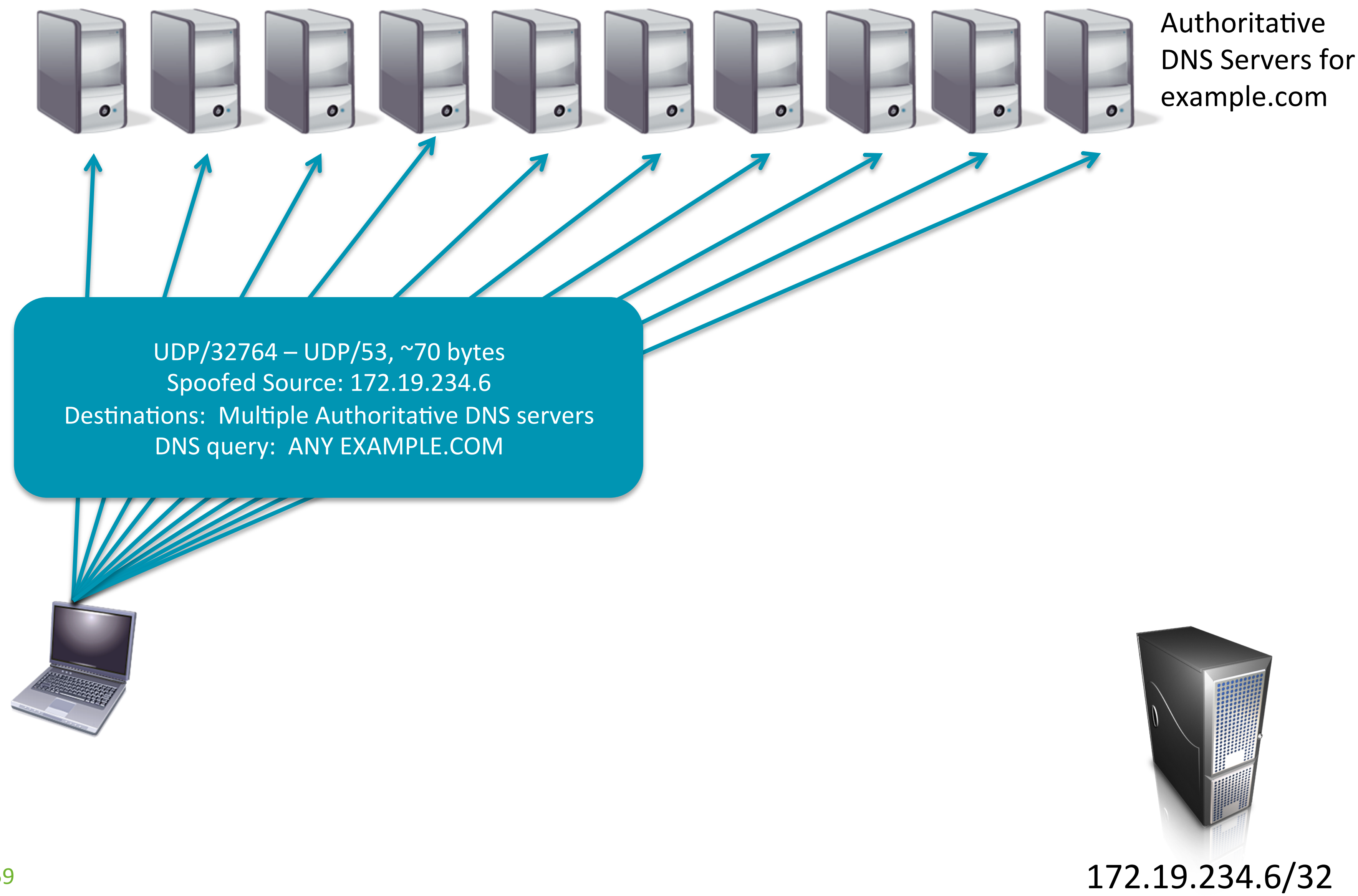
- The attacker spoofs the IP address of the target of the attack, sending DNS queries for pre-identified large DNS records (ANY records, large TXT records, etc.) either to abusable open DNS recursive servers, or directly to authoritative DNS servers.
- The attacker chooses the UDP port which he'd like to target – with DNS, this is typically limited to either UDP/53 or UDP/1024-65535 The destination port is UDP/53
- The servers 'reply' either directly to the attack target or to the intermediate open DNS recursive server with large DNS responses – the attack target will see streams of unsolicited DNS responses broken down into initial and non-initial fragments.
- Response sizes are typically 4096 – 8192 bytes (can be smaller or larger), broken down into multiple fragments.
- Packet sizes received by the attack target are generally ~1500 bytes due to prevalent Ethernet MTUs – and there are lots of them.

Characteristics of a DNS Reflection/Amplification Attack (cont.)

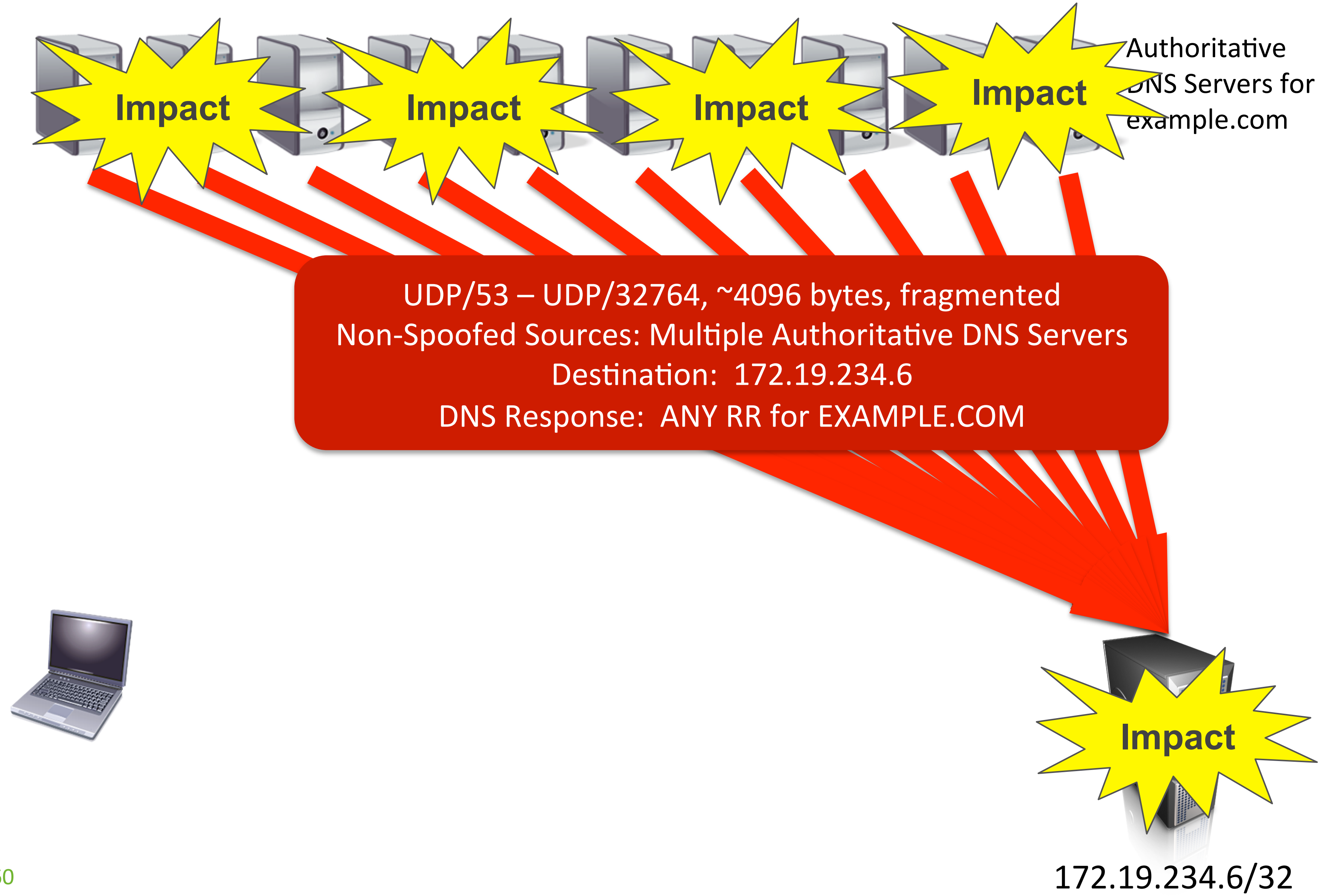
- As these multiple streams of fragmented DNS responses converge, the attack volume can be huge – the largest verified attack of this type so far is ~200gb/sec. 100gb/sec attacks are commonplace.
- Internet transit bandwidth of the target, along with core bandwidth of the target's peers/upstreams, as well as the core bandwidth of intermediary networks between the various DNS services being abused and the target, are saturated.
- In most attacks involving intermediate open DNS recursive servers are reflectors, between ~20,000 – 30,000 abusable recursive DNS are leveraged by attackers. Up to 50,000 abusable open recursive DNS servers have been observed in some attacks.
- In attacks leveraging authoritative DNS servers directly, hundreds or thousands of these servers are utilized by attackers.
- Many well-known authoritative DNS servers are anycasted, with multiple instances deployed around the Internet.

DNS Reflection/Amplification Attack Methodology #1

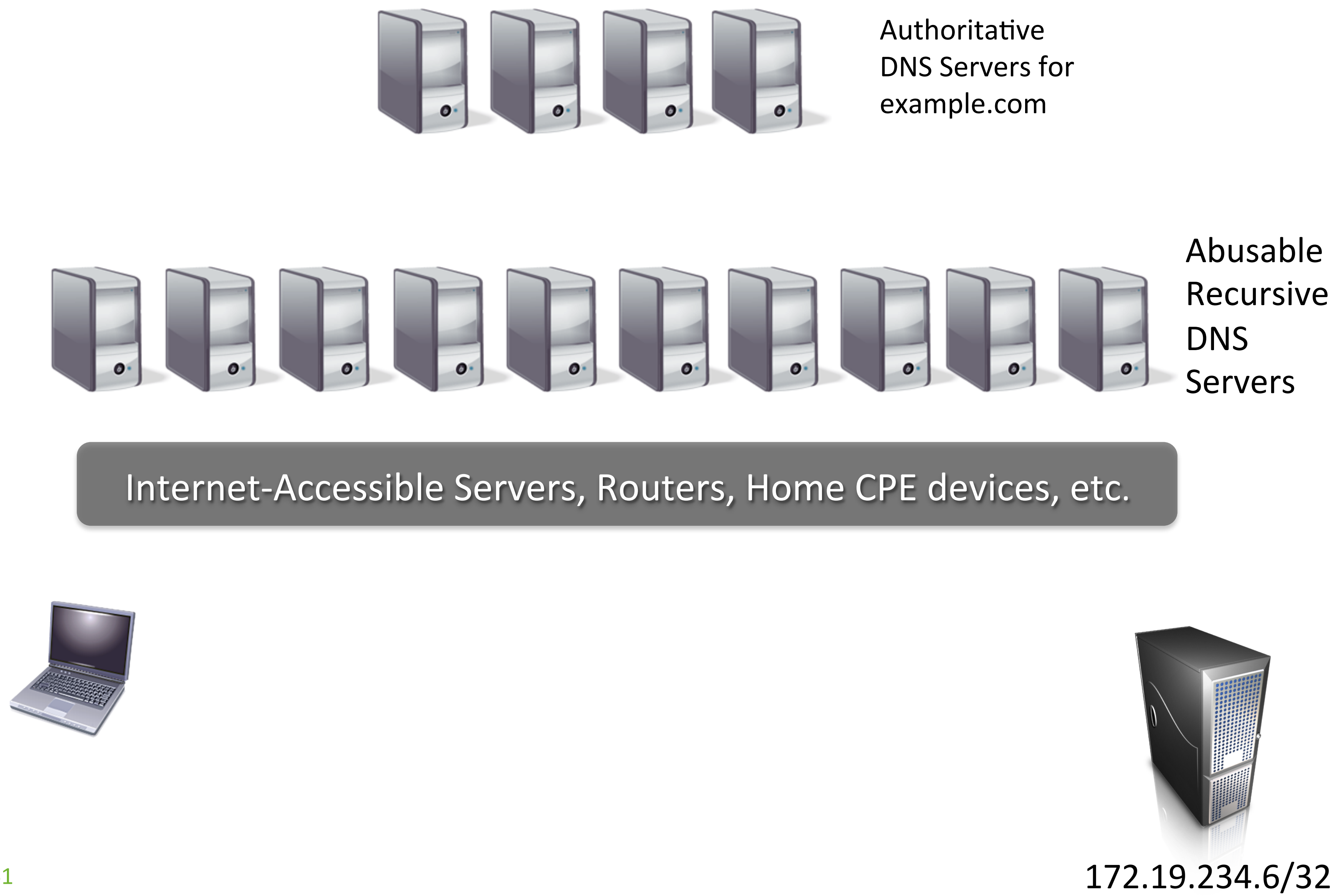
DNS Reflection/Amplification Attack Methodology #1



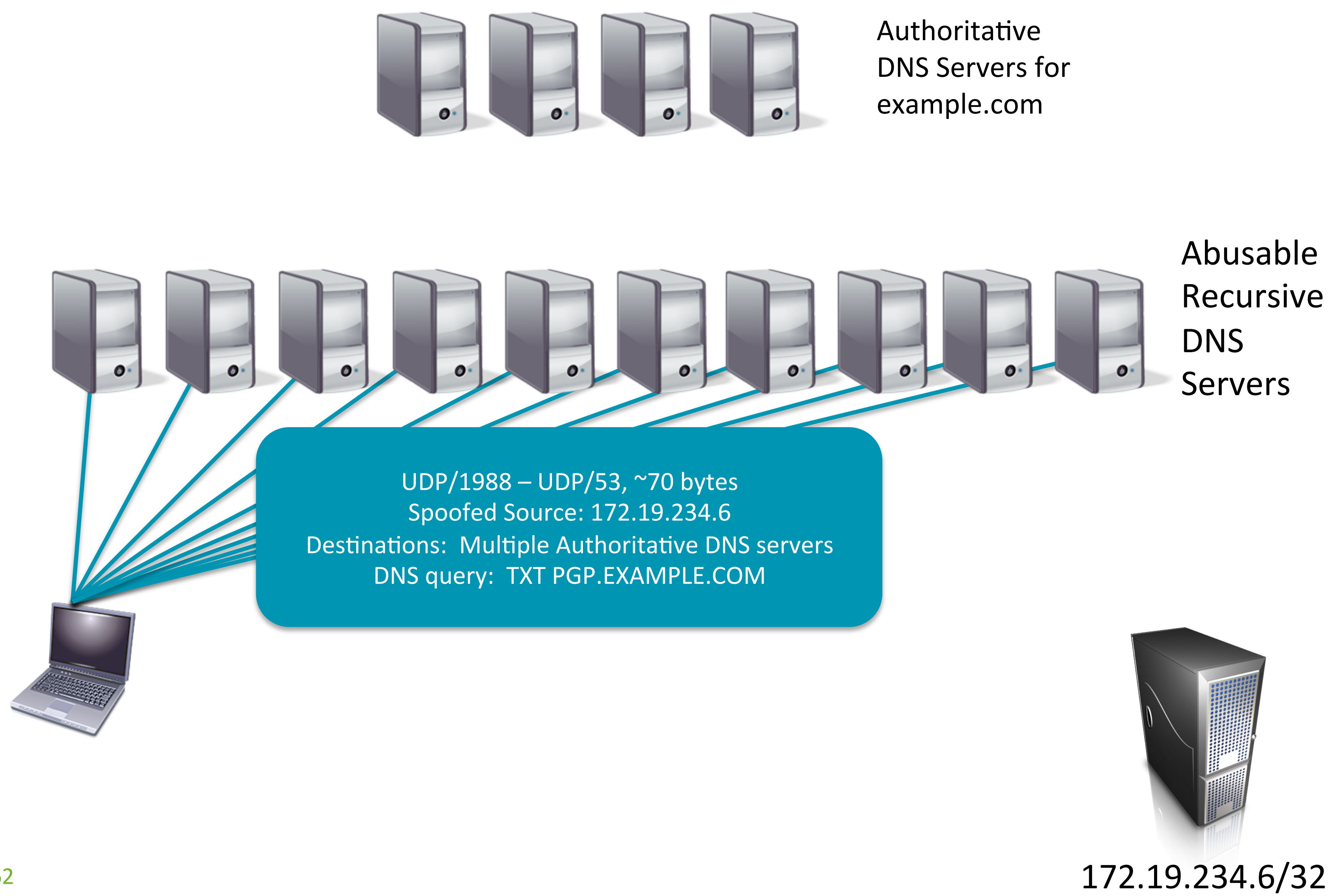
DNS Reflection/Amplification Attack Methodology #1



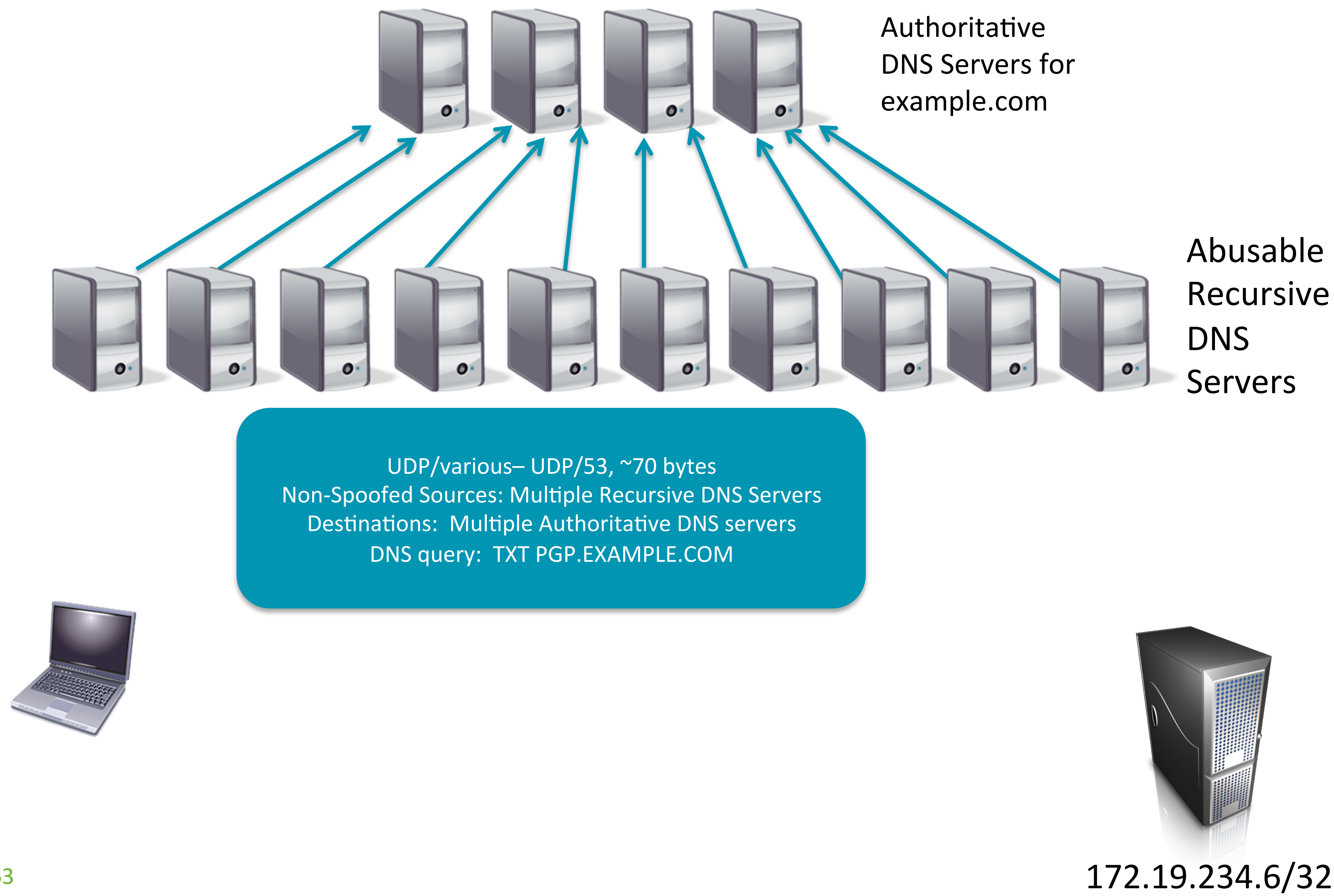
DNS Reflection/Amplification Attack Methodology #2



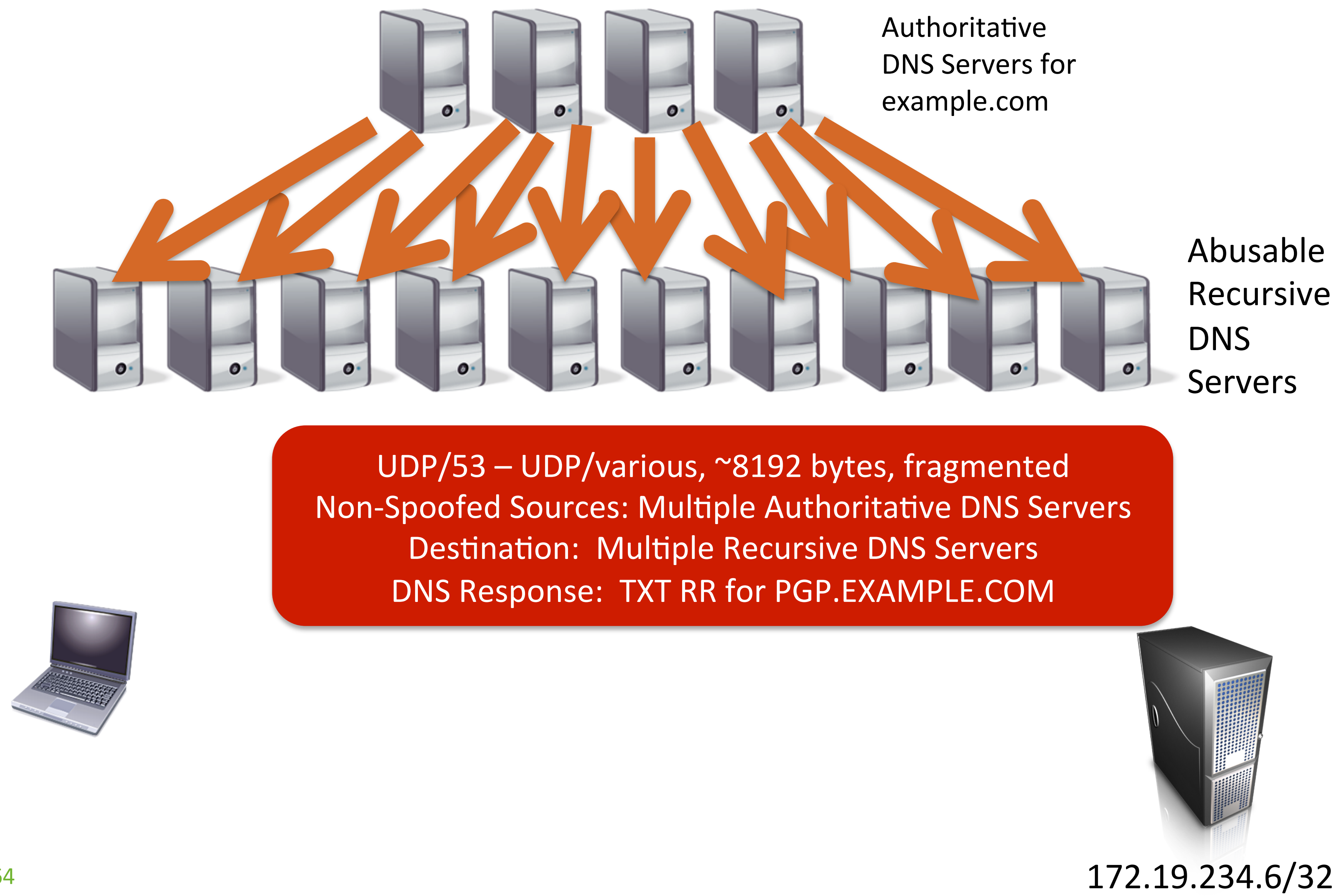
DNS Reflection/Amplification Attack Methodology #2



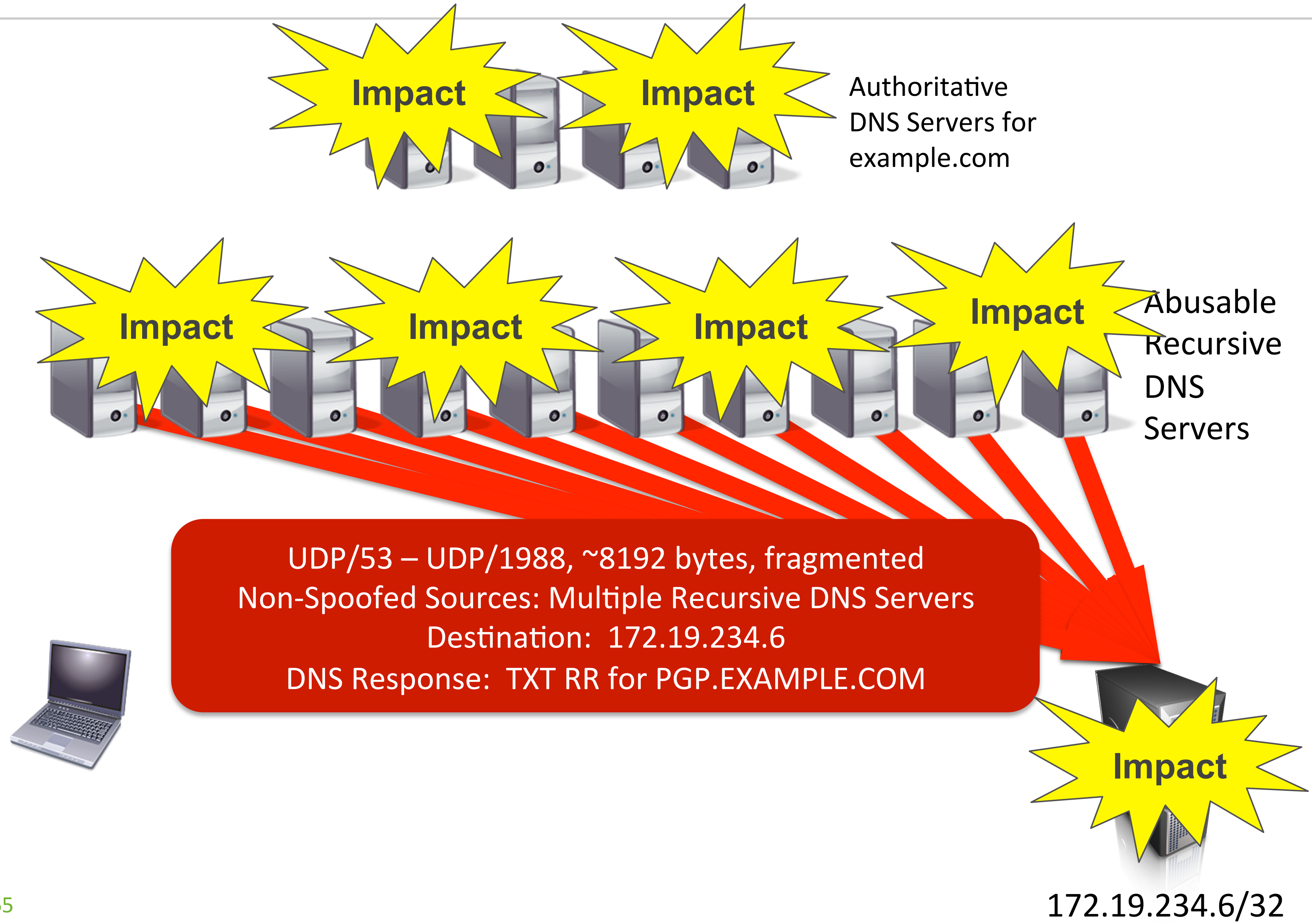
DNS Reflection/Amplification Attack Methodology #2



DNS Reflection/Amplification Attack Methodology #2

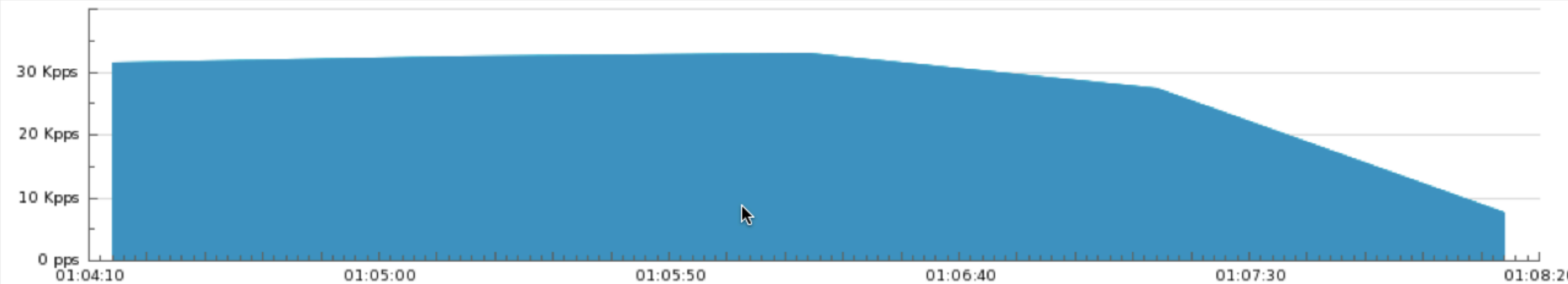


DNS Reflection/Amplification Attack Methodology #2



DNS Reflection/Amplification Attack – UDP/53

DoS Alert 1077616 | **Classification:** Possible Attack | **Apr 4 01:03 - 01:12 (0:09)**



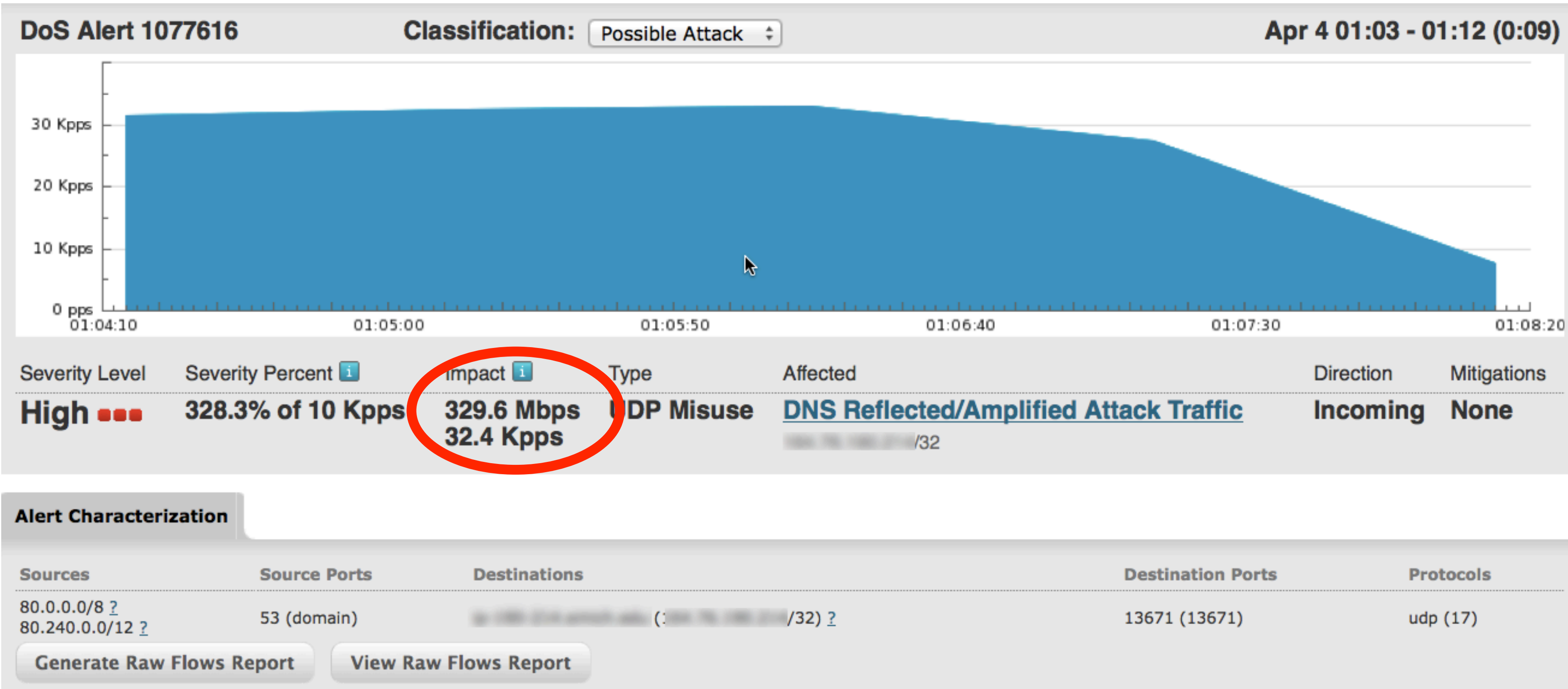
Severity Level	Severity Percent	Impact	Type	Affected	Direction	Mitigations
High	**328.3% of 10 Kpps**	**329.6 Mbps** **32.4 Kpps**	**UDP Misuse**	**DNS Reflected/Amplified Attack Traffic** [illegible]/32	**Incoming**	**None**

Alert Characterization

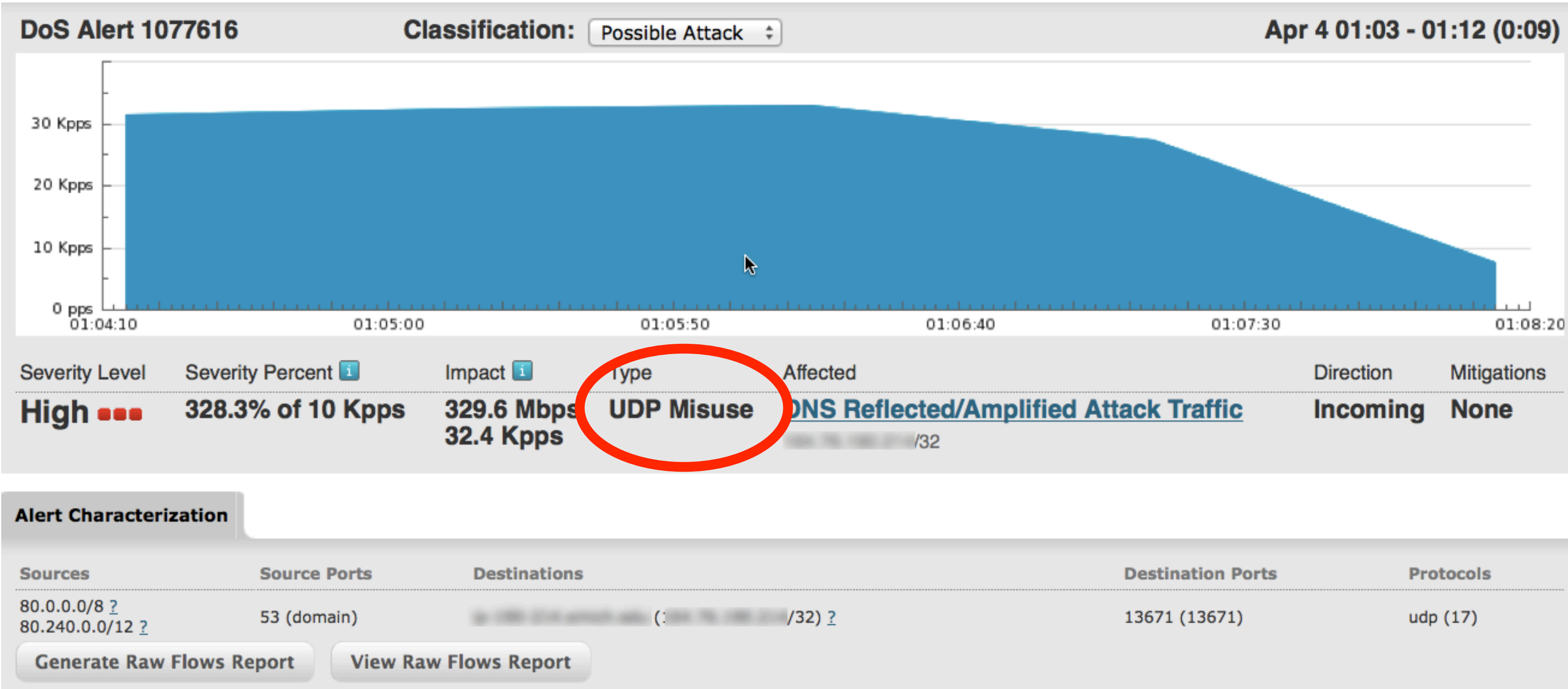
Sources	Source Ports	Destinations	Destination Ports	Protocols
80.0.0.0/8 ? 80.240.0.0/12 ?	53 (domain)	[illegible] ([illegible]/32) ?	13671 (13671)	udp (17)

Generate Raw Flows Report | View Raw Flows Report

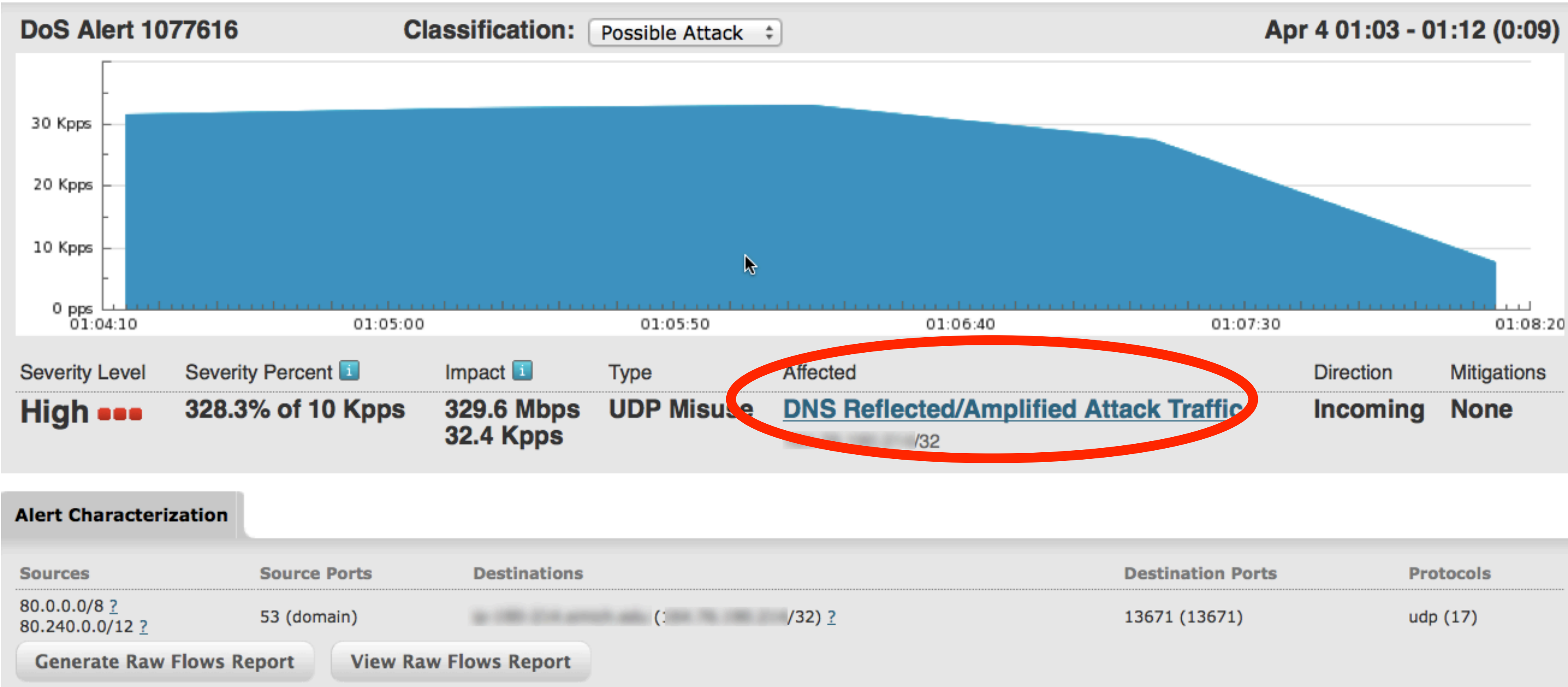
DNS Reflection/Amplification Attack – UDP/53



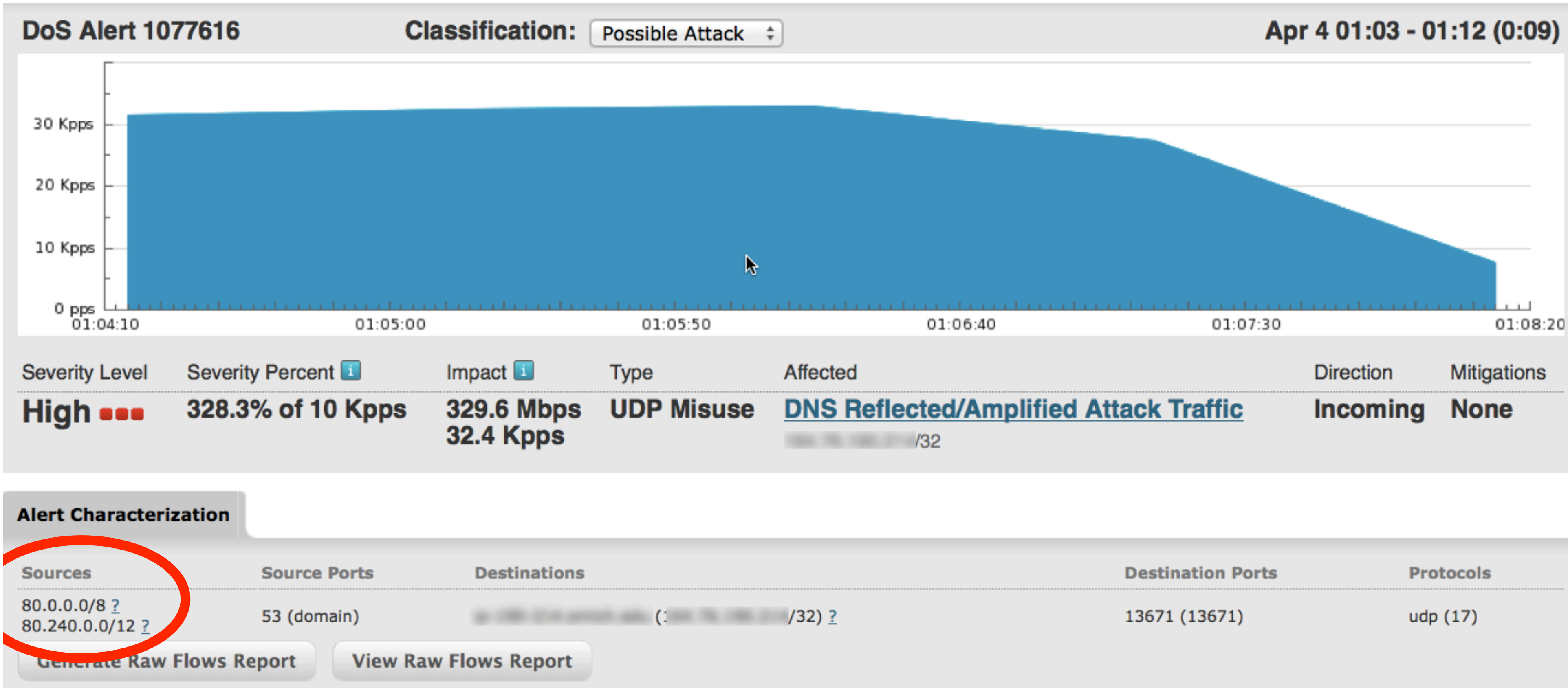
DNS Reflection/Amplification Attack – UDP/53



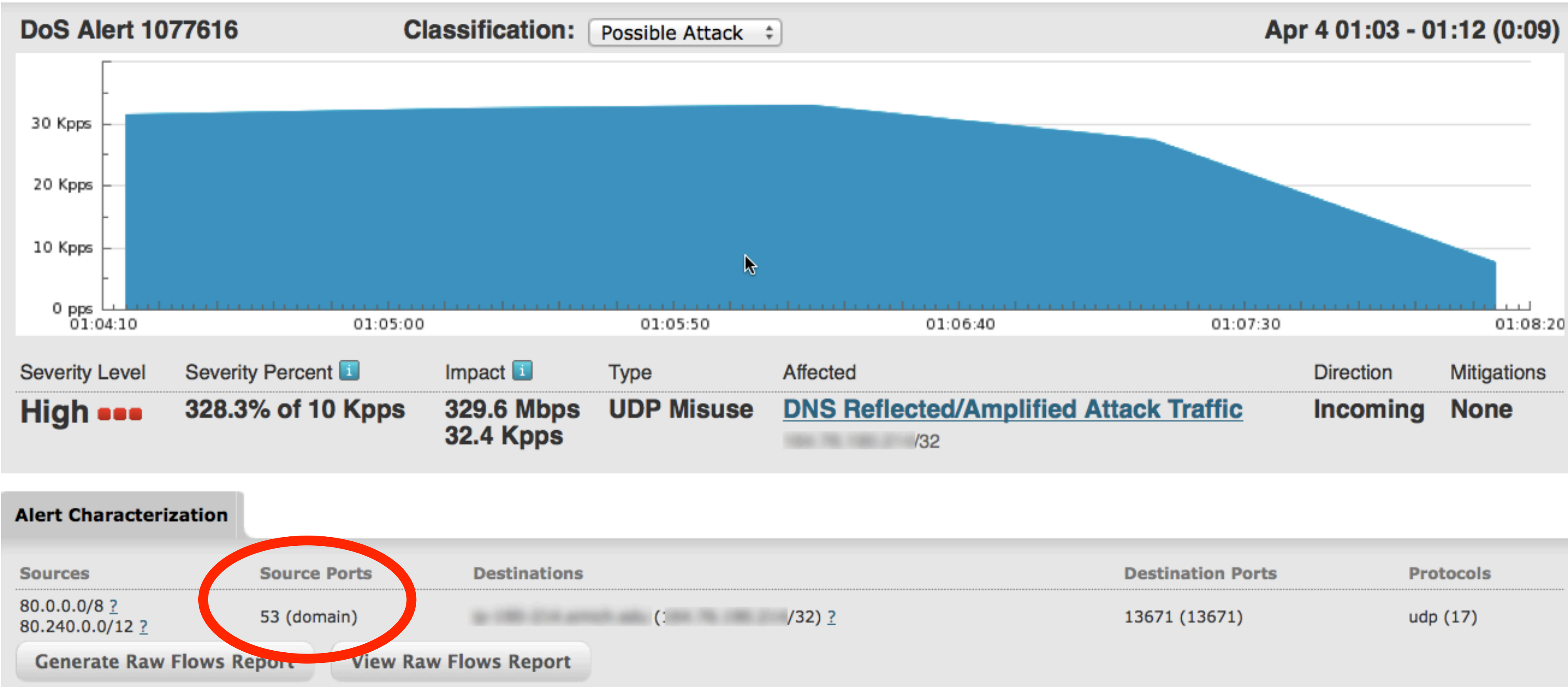
DNS Reflection/Amplification Attack – UDP/53



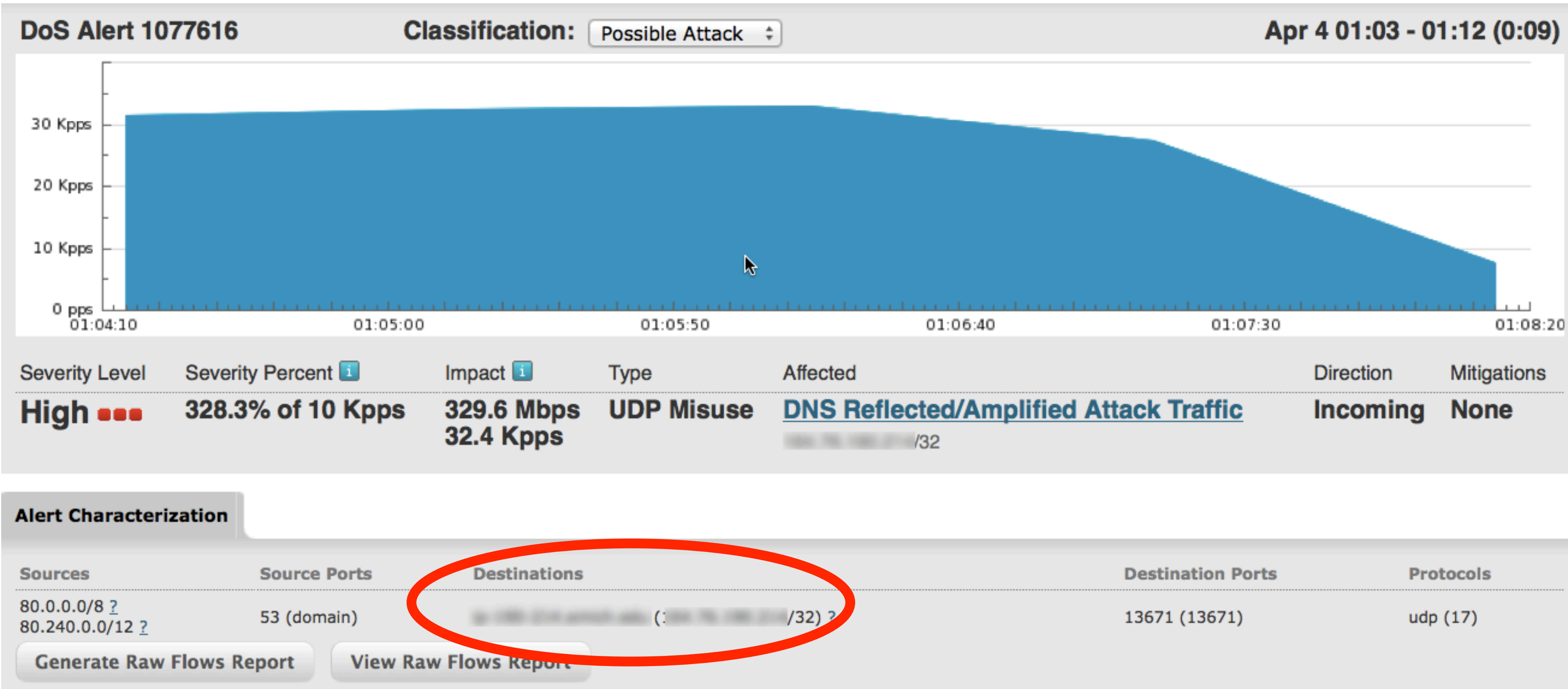
DNS Reflection/Amplification Attack – UDP/53



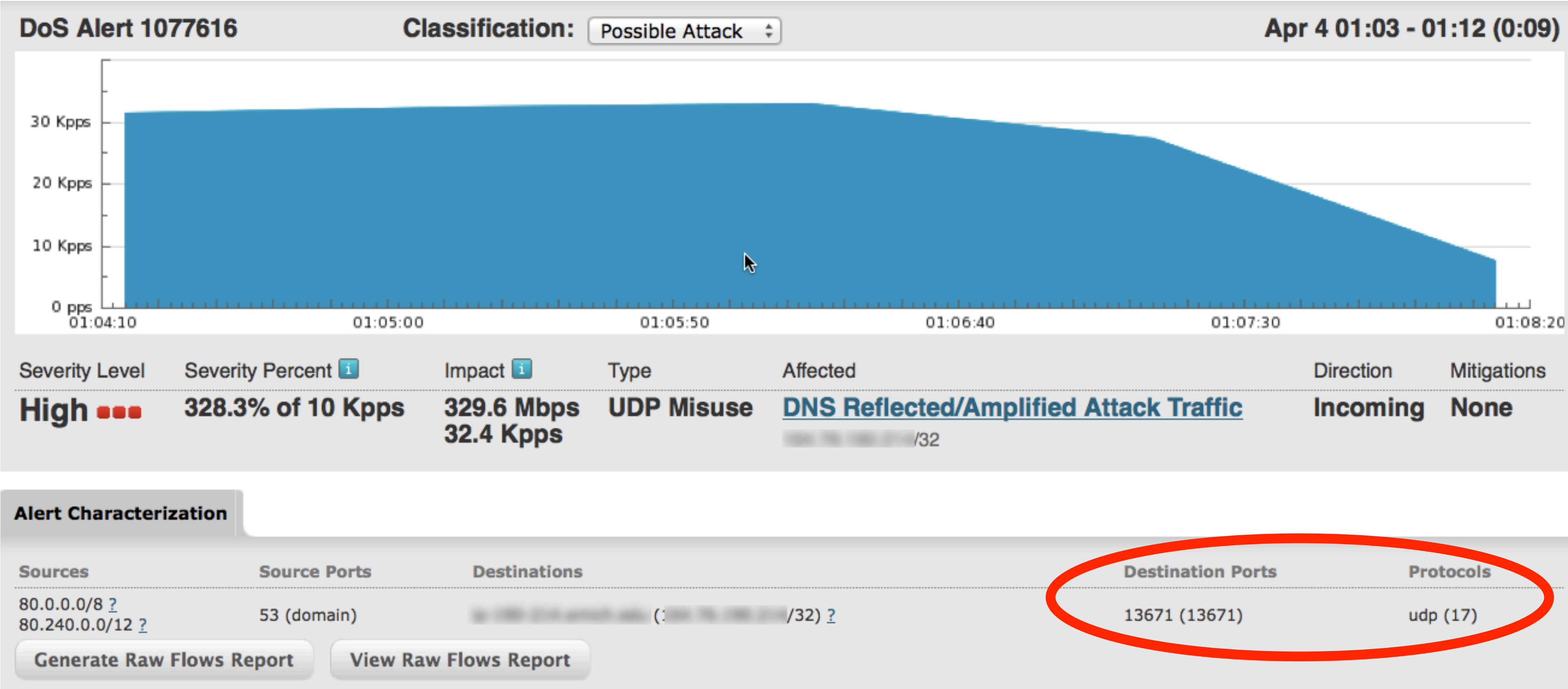
DNS Reflection/Amplification Attack – UDP/53



DNS Reflection/Amplification Attack – UDP/53



DNS Reflection/Amplification Attack – UDP/53



DNS Reflection/Amplification Attack – 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.

DNS Reflection/Amplification Attack – 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.

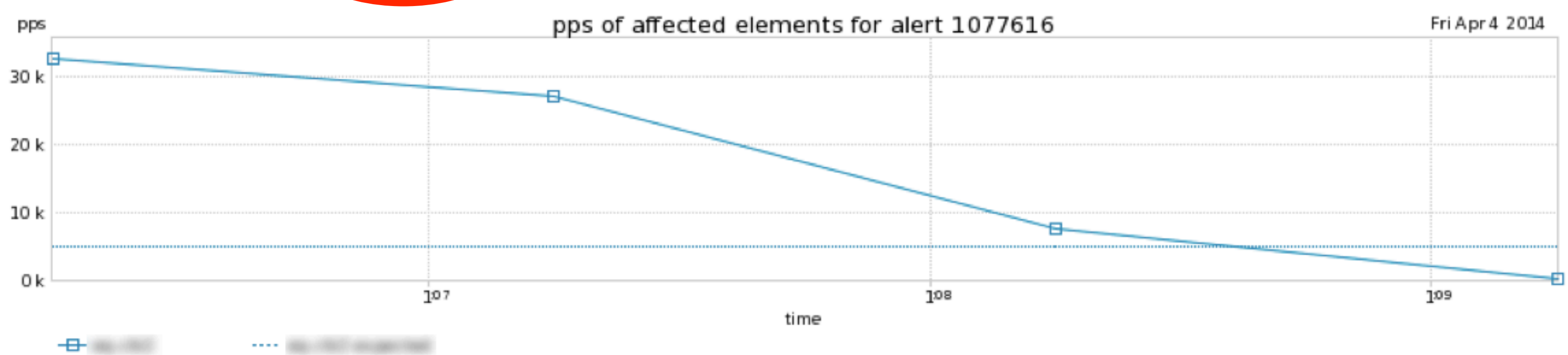
DNS Reflection/Amplification Attack – UDP/53

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 [illegible]/32 DNS Reflected/Amplified Attack Traffic



DNS Reflection/Amplification Attack – UDP/53

Affected Network Elements

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

Change Timeframe

Timeframe:

Interval	Start	End
Other	2014-04-04 01:06:15	2014-04-04 01:09:15

Update

Traffic Details for router

Summary

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

DNS Reflection/Amplification Attack – 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	☑

DNS Reflection/Amplification Attack – 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	☑

DNS Reflection/Amplification Attack – 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	☑

DNS Reflection/Amplification Attack – UDP/53

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[illegible] ([illegible] /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	☑

DNS Reflection/Amplification Attack – UDP/53

Destination Addresses

Address/Mask	Bytes	Packets	Bytes/Pkt	bps	pps	% pps	Filter
[illegible] ([illegible]/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	☑

DNS Reflection/Amplification Attack – 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	☑

DNS Reflection/Amplification Attack – 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	☑

DNS Reflection/Amplification Attack – 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
x[illegible]-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	☑
[illegible]e-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	☑

DNS Reflection/Amplification Attack – 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	☑

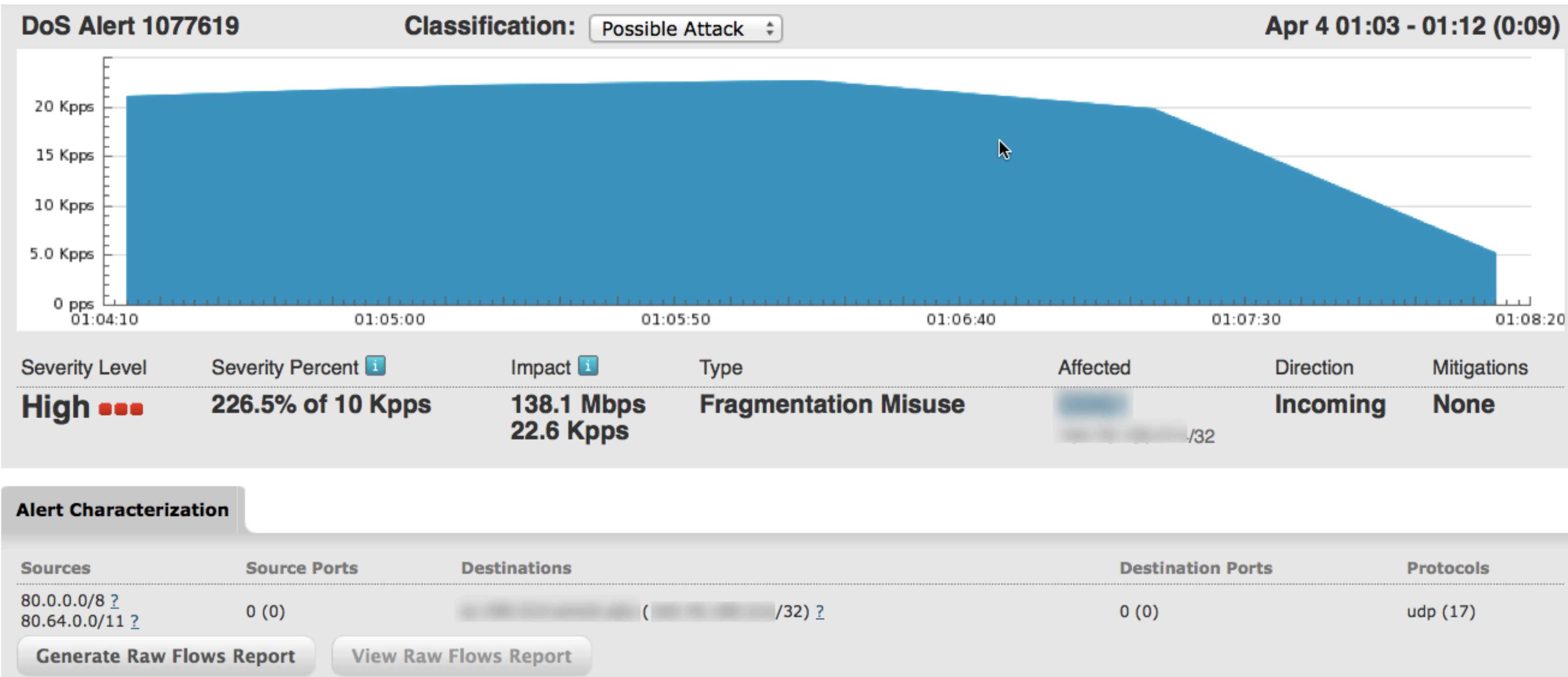
Ingress Interfaces

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	☐

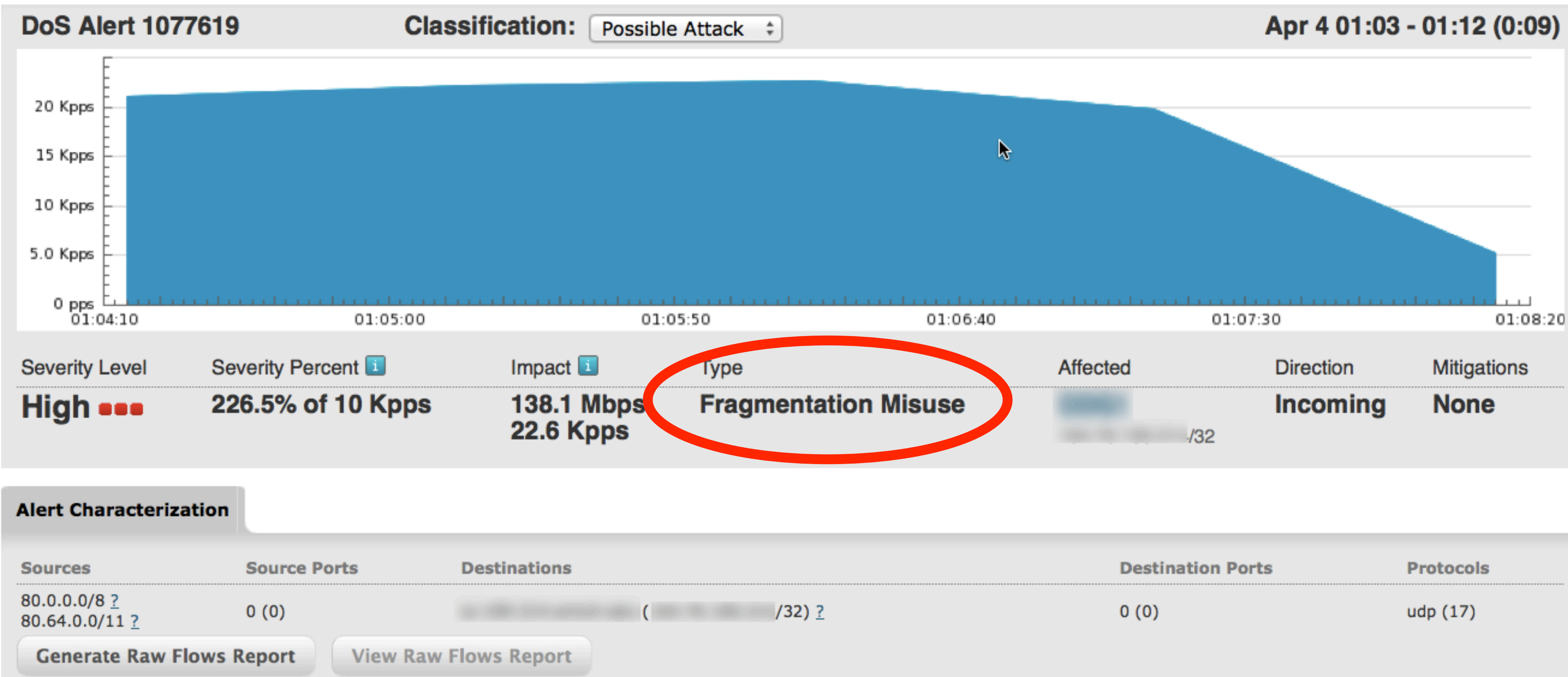
Egress Interfaces

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	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments



DNS Reflection/Amplification Attack – Non-Initial Fragments



DNS Reflection/Amplification Attack – Non-Initial Fragments

Affected Routers

			Observed bps		Observed pps		
	Severity Level	Expected	Max	Overall	Max	Overall	Details
Router [illegible]	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 [illegible]		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584 [illegible]		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106 [illegible]		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104 [illegible]		-	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.

DNS Reflection/Amplification Attack – Non-Initial Fragments

Affected Routers

	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	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		-	1.98 Mbps	1.27 Mbps	300.00 pps	188.89 pps	Details
Interface (SNMP 518) xe-5/0/1.584		-	2.18 Mbps	1.29 Mbps	383.00 pps	200.00 pps	Details
Interface (SNMP 521) xe-5/1/0.106		-	79.11 Mbps	53.43 Mbps	13.18 Kpps	8.89 Kpps	Details
Interface (SNMP 584) xe-4/0/0.104		-	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.

DNS Reflection/Amplification Attack – Non-Initial Fragments

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	15.36 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.

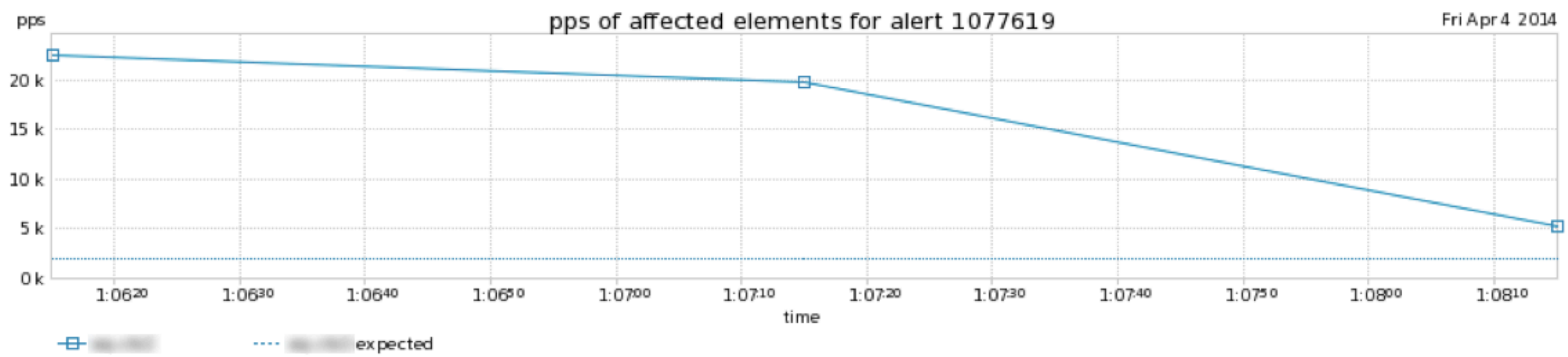
DNS Reflection/Amplification Attack – Non-Initial Fragments

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)	/32



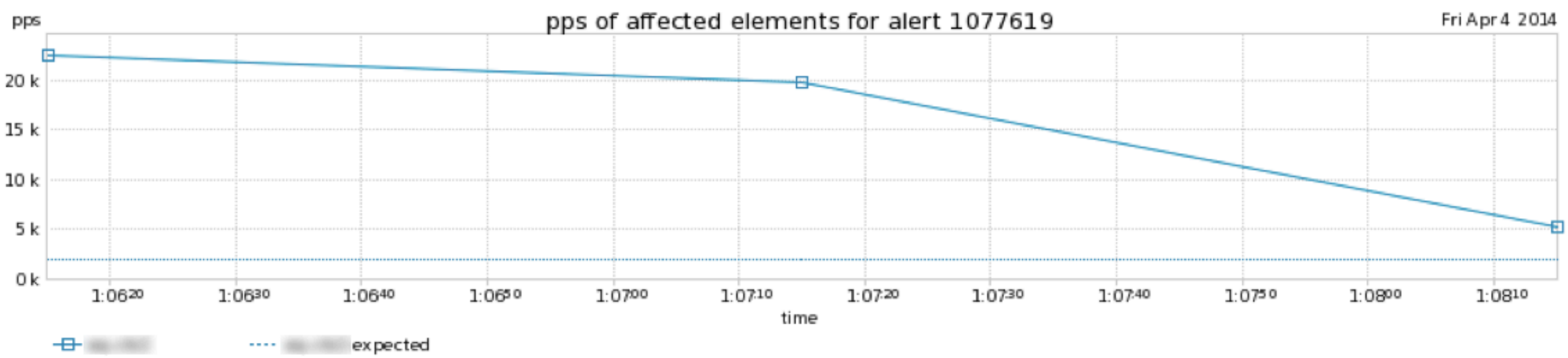
DNS Reflection/Amplification Attack – Non-Initial Fragments

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)	[illegible]/32



DNS Reflection/Amplification Attack – Non-Initial Fragments

Affected Network Elements

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

Change Timeframe

Timeframe:

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

Traffic Details for router [illegible]

Summary

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

DNS Reflection/Amplification Attack – Non-Initial Fragments

Affected Network Elements

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

Change Timeframe

Timeframe:

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

Traffic Details for router

Summary

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

DNS Reflection/Amplification Attack – Non-Initial Fragments

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
[illegible] ([illegible]/32) ?	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments

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
[illegible] ([illegible]/32) ?	2.16 G	2.86 M	757.78	96.15 M	15.86 k	100.00	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments

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	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments

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	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments

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	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments

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	☑

DNS Reflection/Amplification Attack – Non-Initial Fragments

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	☑

SNMP Reflection/Amplification

Amplification Factor - SNMP

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

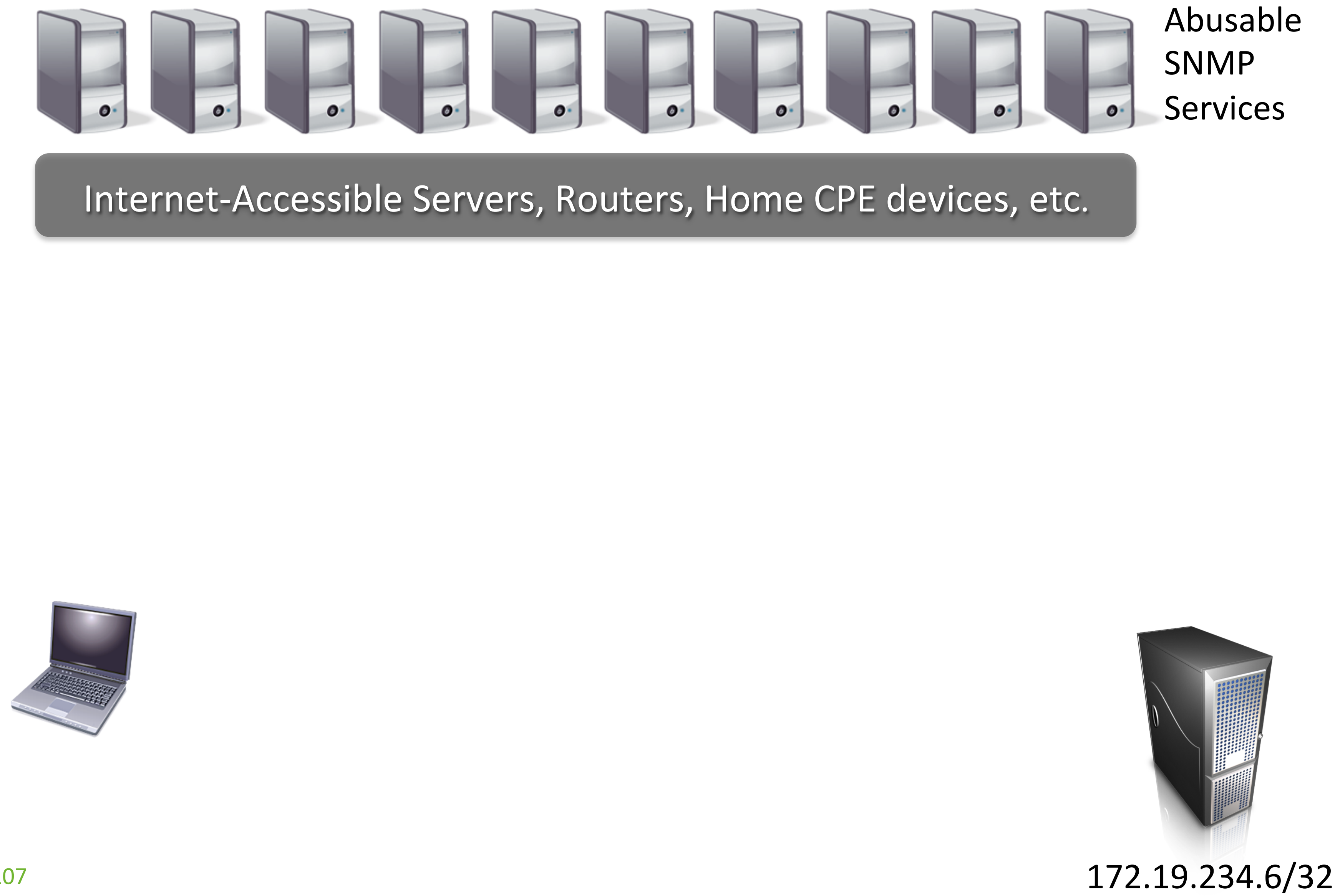
Characteristics of an SNMP Reflection/Amplification Attack

- The attacker spoofs the IP address of the target of the attack, sends an SNMP *GetBulkRequest* query to abusable SNMP services running on home CPE devices, large ISP and enterprise routers, servers, etc. These packets are typically between 60 – 102 bytes in length
- The attacker chooses the UDP port which he'd like to target – it can be any port of the attacker's choice – and uses that as the source port. The destination port is UDP/161.
- The SNMP services 'reply' to the attack target with streams of 423-byte – 1560-byte packets sourced from UDP/161; the destination port is the source port the attacker chose when generating the SNMP queries.

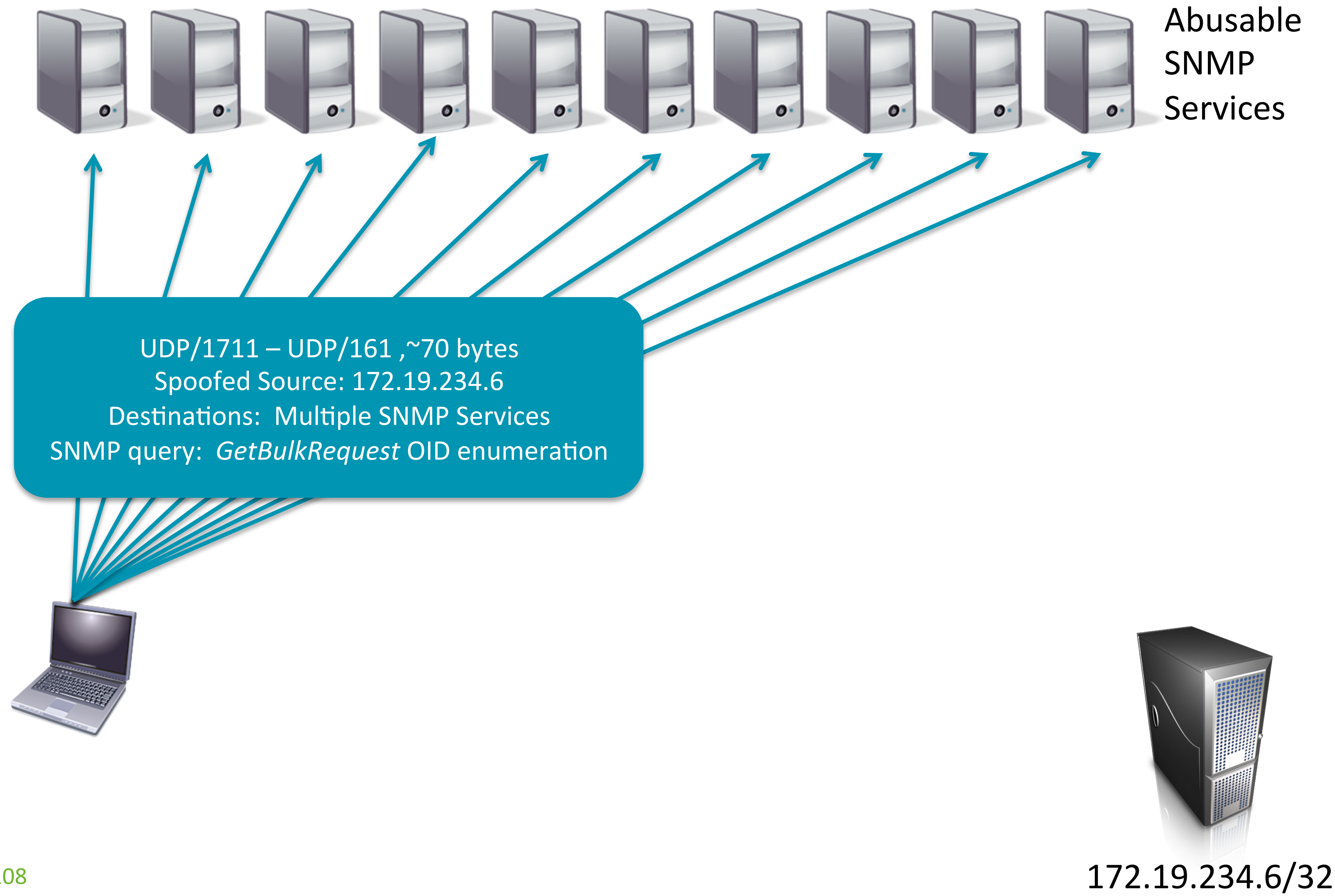
Characteristics of an SNMP Reflection/Amplification Attack (cont.)

- As these multiple streams of SNMP replies converge, the attack volume can be very large – the largest verified attack of this type so far is over 60gb/sec. 20-30gb/sec attacks are commonplace.
- Due to sheer attack volume, the Internet transit bandwidth of the target, along with core bandwidth of the target's peers/upstreams, as well as the core bandwidth of intermediary networks between the various SNMP services being abused and the target, are saturated.
- More savvy attackers will enumerate the individual SNMP Object IDentifiers (OIDs) on the abusable SNMP services, and enumerate each one with iterative parallel spoofed SNMP queries. Lots of non-initial fragments in this scenario, a la DNS.
- In most attacks, between ~2,000-4,000 abusable SNMP services are leveraged by attackers. Up to 10,000 SNMP services have been observed in some attacks.

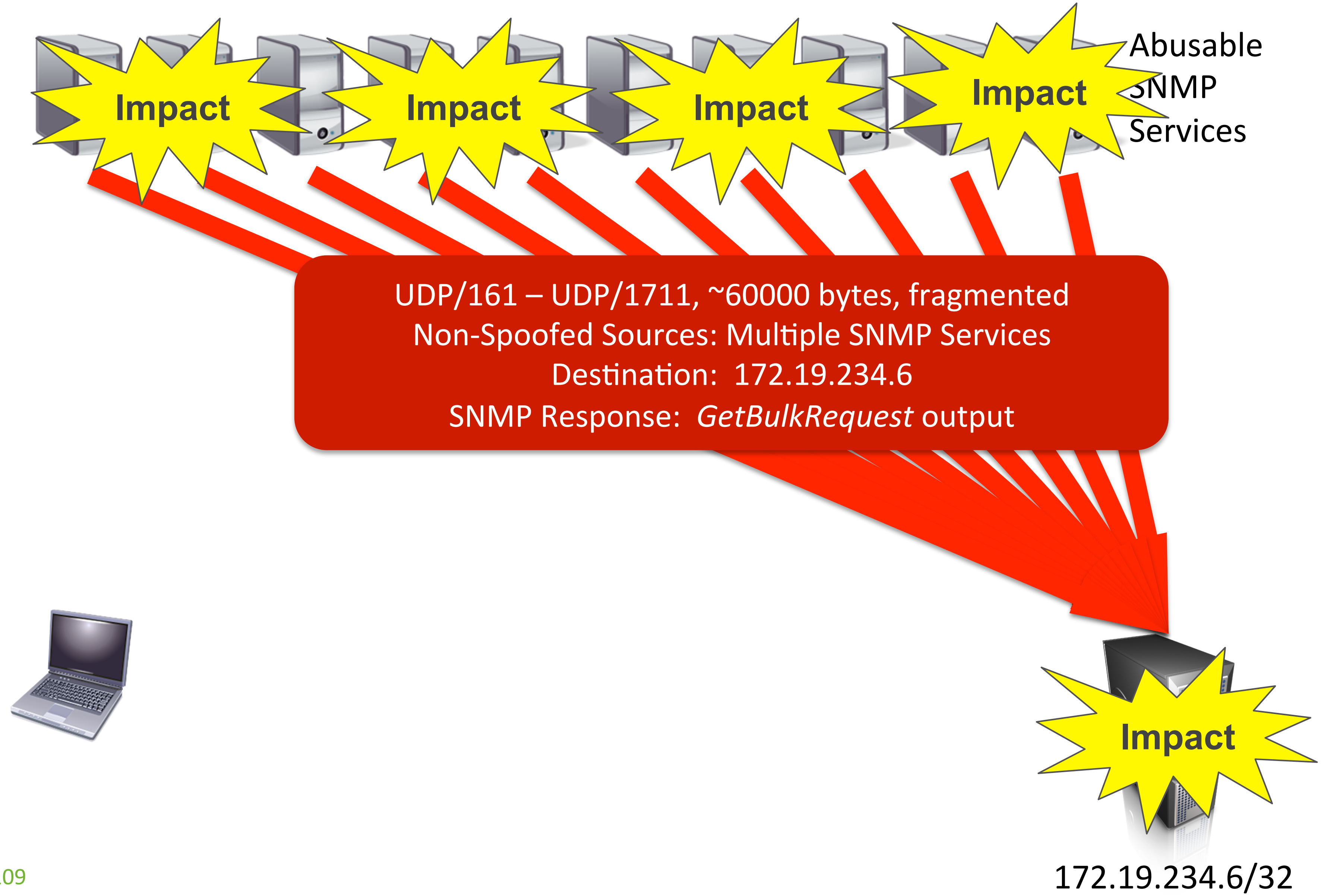
SNMP Reflection/Amplification Attack Methodology



SNMP Reflection/Amplification Attack Methodology



SNMP Reflection/Amplification Attack Methodology



chargen Reflection/Amplification

Amplification Factor - chargen

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

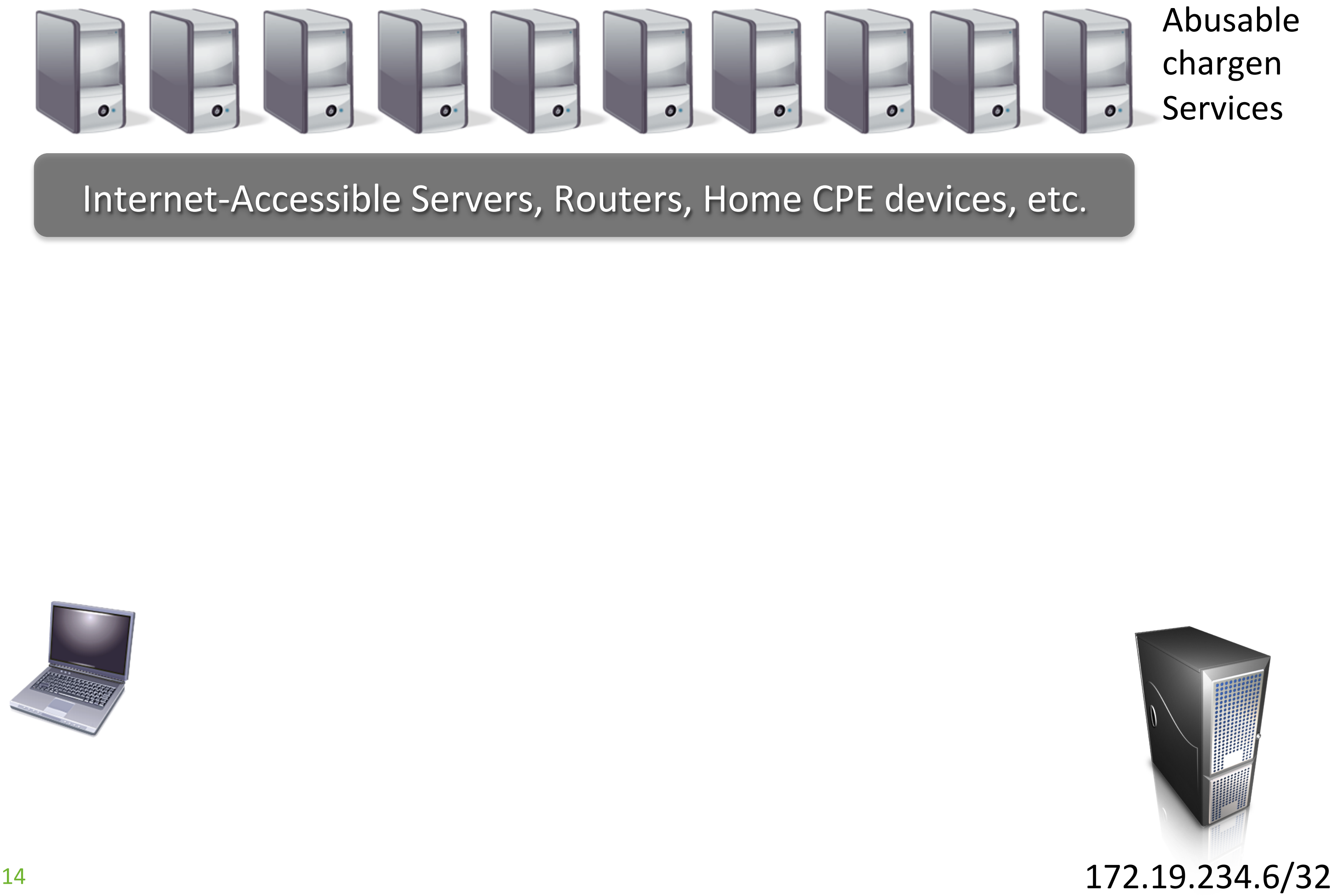
Characteristics of a chargen Reflection/Amplification Attack

- The attacker spoofs the IP address of the target of the attack, sends packets padded with at least 18 bytes of payload (all-zeroes; 70-byte packet) to multiple abusable chargen services running on servers, printers, home CPE devices, etc.
- The attacker chooses the UDP port which he'd like to target – it can be any port greater than 1023 – and uses that as the source port. The destination port is UDP/19.
- The chargen services 'reply' to the attack target with ~1000-byte - ~1500-bytes packets sourced from UDP/19 to the target; the destination port is the source port the attacker chose when he generated the chargen queries. Most chargen services generate one response packet for each request packets, but some non-RFC-compliant chargen services send more packets/query.

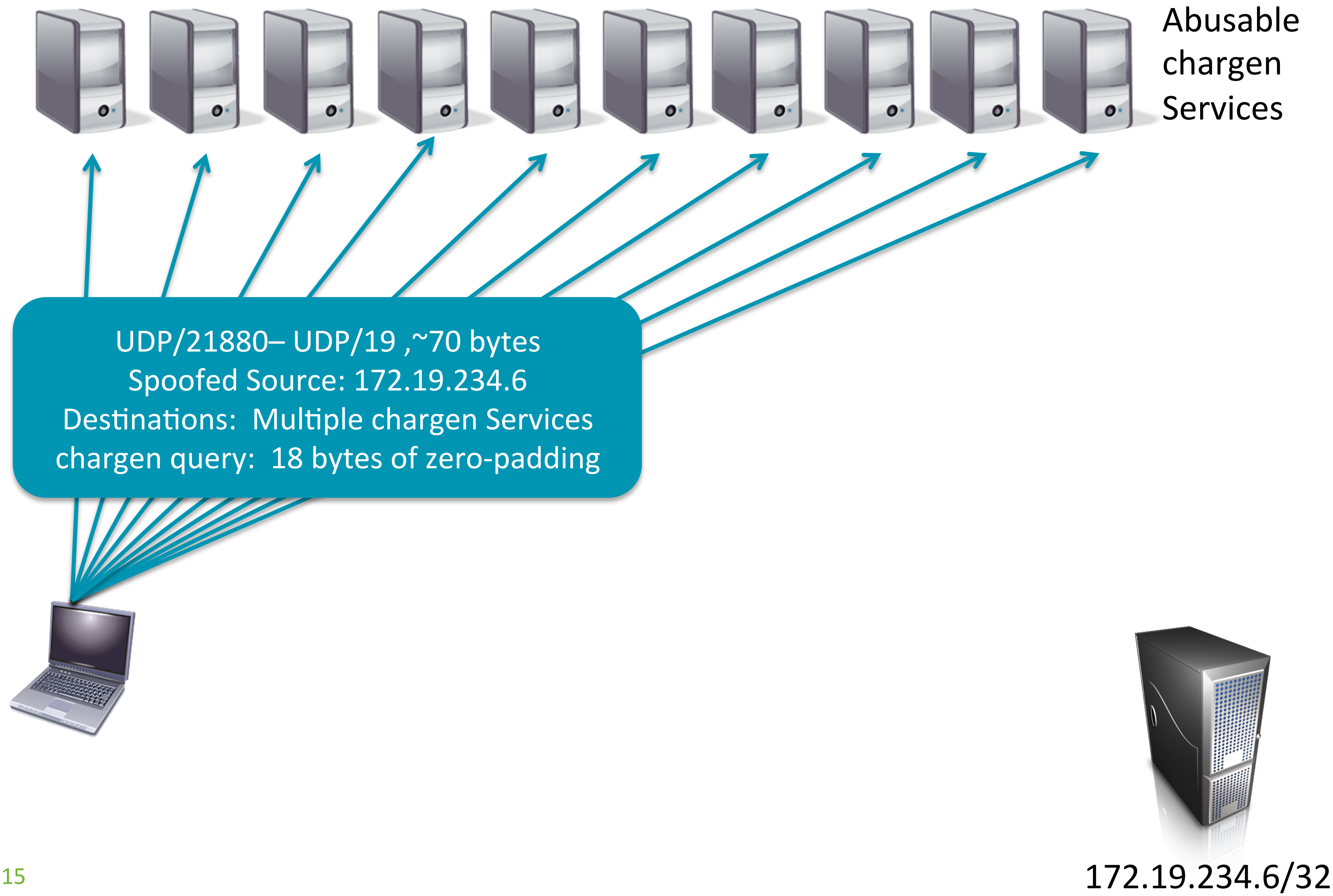
Characteristics of a chargen Reflection/Amplification Attack (cont.)

- As these multiple streams of chargen replies converge, the attack volume can be quite large – the largest verified attack of this type so far is over 137gb/sec. 2-5gb/sec attacks are commonplace.
- Due to sheer attack volume, the Internet transit bandwidth of the target, along with core bandwidth of the target's peers/ upstreams, as well as the core bandwidth of intermediary networks between the various chargen services being abused and the target, can be saturated.
- Non-RFC-compliant chargen services can provide an amplification factor of up to 1000:1 (most are 18:1).
- In most attacks, between ~20 - ~2,000 abusable chargen services are leveraged by attackers. Up to 5,000 chargen services have been observed in some attacks.

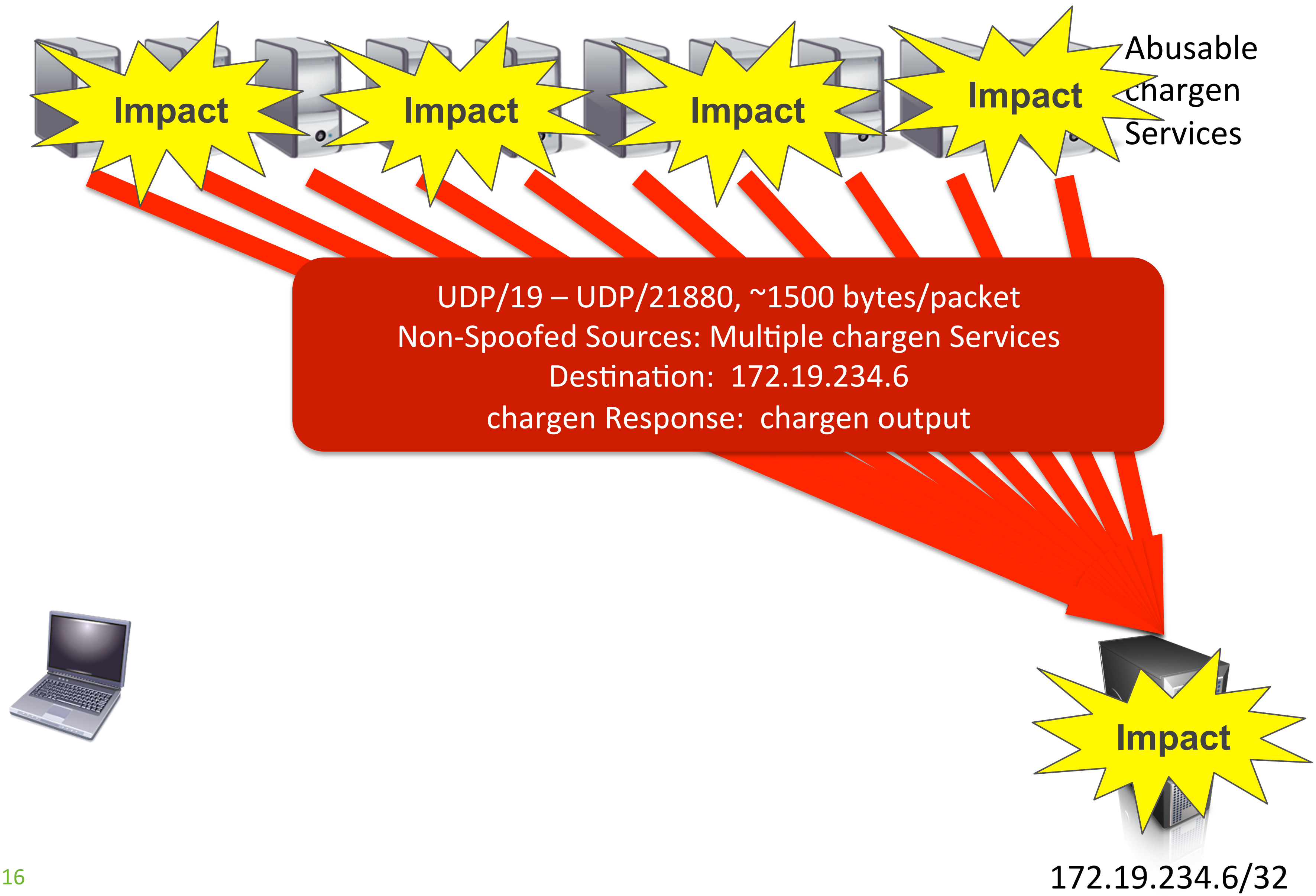
chargen Reflection/Amplification Attack Methodology



chargen Reflection/Amplification Attack Methodology

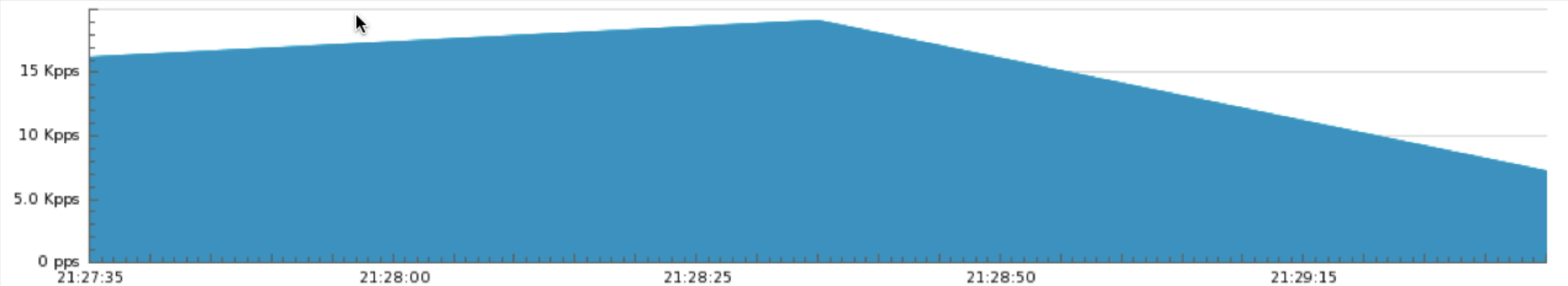


chargen Reflection/Amplification Attack Methodology



chargen Reflection/Amplification Attack – UDP/19

DoS Alert 1078798 **Classification:** Verified Attack **Apr 6 21:26 - 21:33 (0:07)**



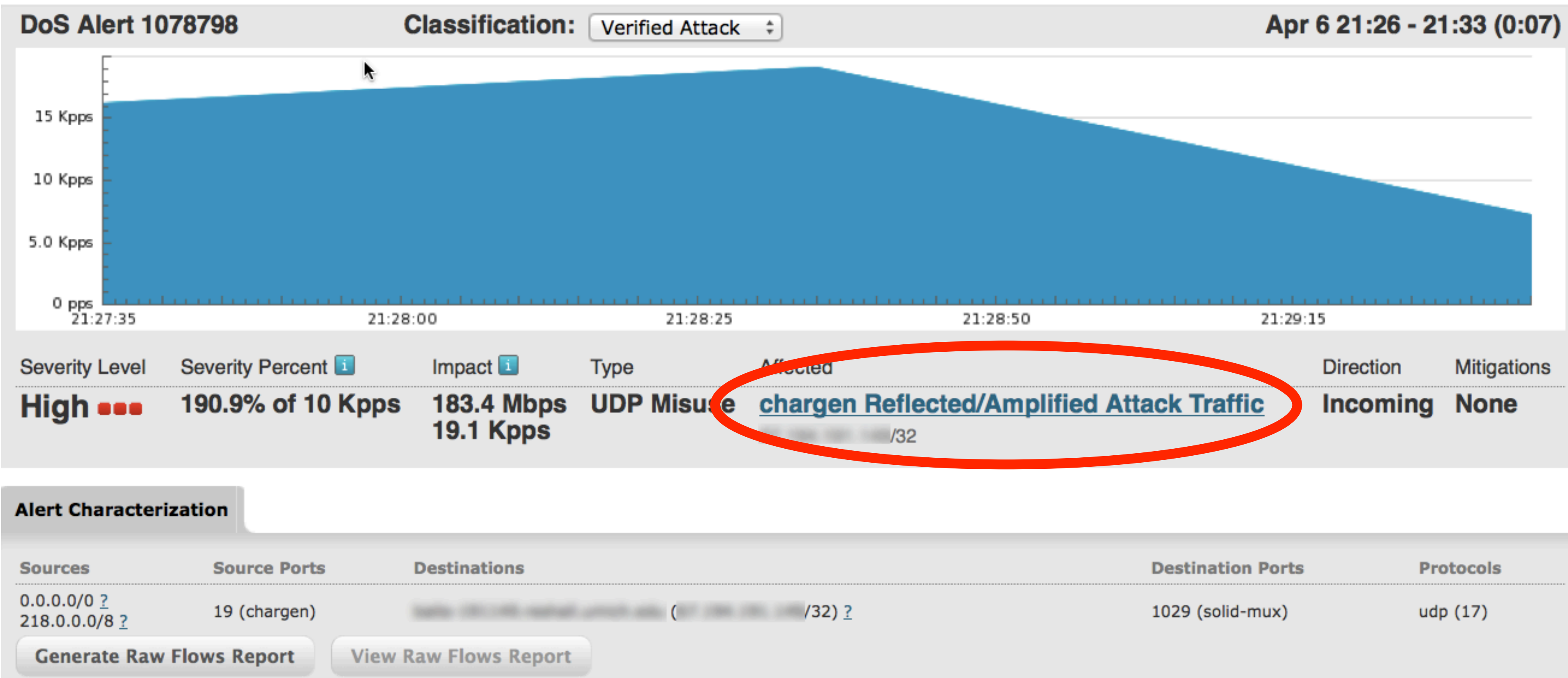
Severity Level	Severity Percent	Impact	Type	Affected	Direction	Mitigations
High	**190.9% of 10 Kpps**	**183.4 Mbps 19.1 Kpps**	**UDP Misuse**	**chargen Reflected/Amplified Attack Traffic** [illegible]/32	**Incoming**	**None**

Alert Characterization

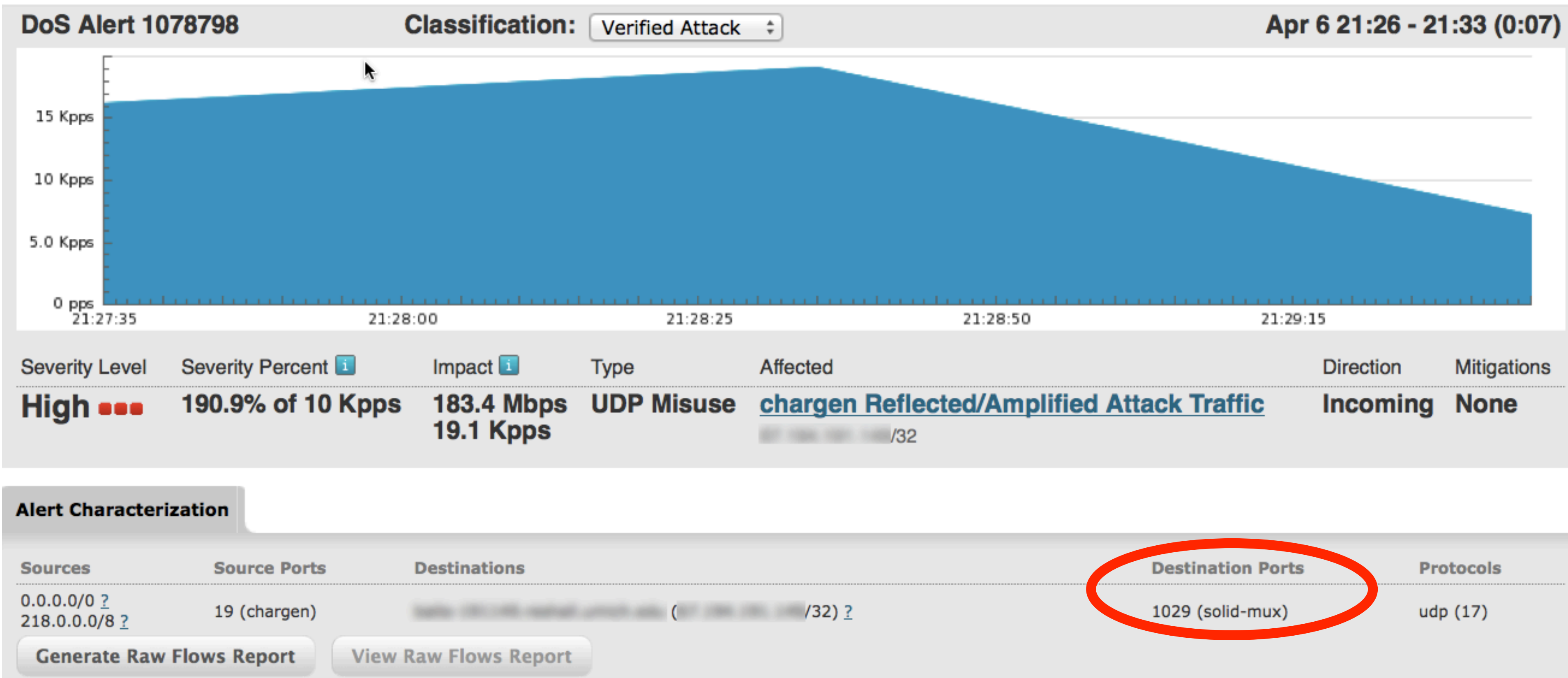
Sources	Source Ports	Destinations	Destination Ports	Protocols
0.0.0.0/0 ? 218.0.0.0/8 ?	19 (chargen)	[illegible] ([illegible]/32) ?	1029 (solid-mux)	udp (17)

Generate Raw Flows Report | View Raw Flows Report

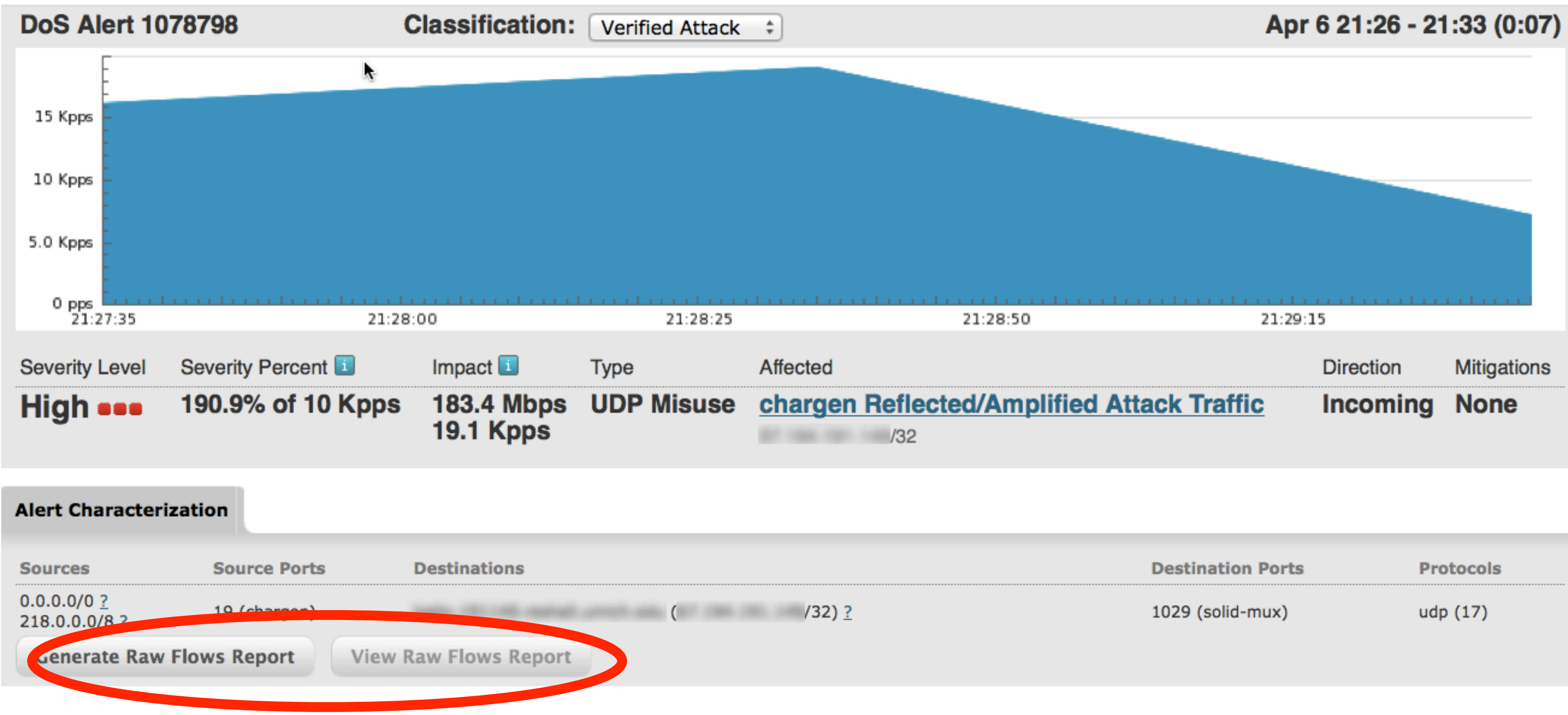
chargen Reflection/Amplification Attack – UDP/19



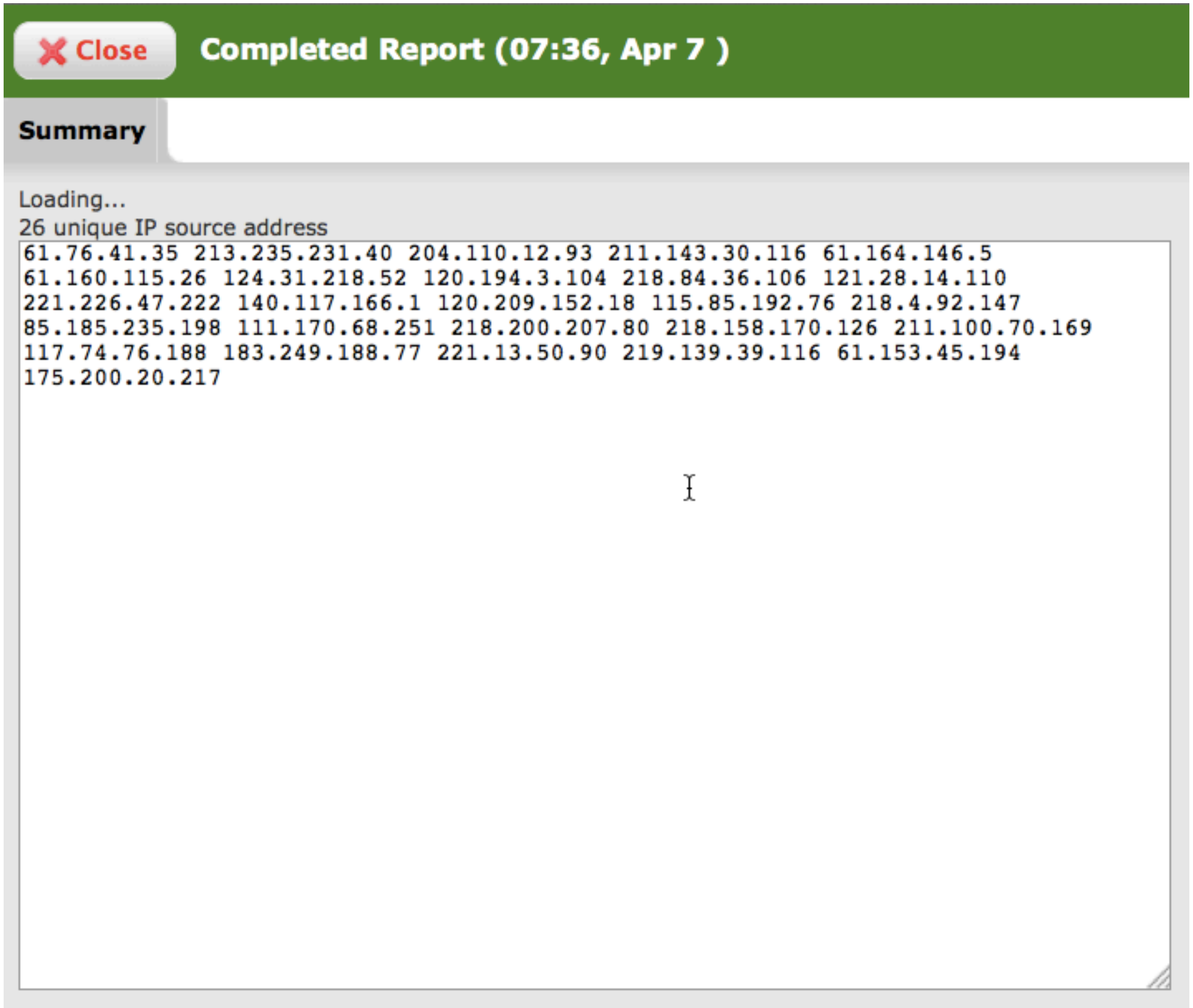
chargen Reflection/Amplification Attack – UDP/19



chargen Reflection/Amplification Attack – UDP/19



chargen Reflection/Amplification Attack – UDP/19



chargen Reflection/Amplification Attack – 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.

chargen Reflection/Amplification Attack – 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.[illegible]6 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.

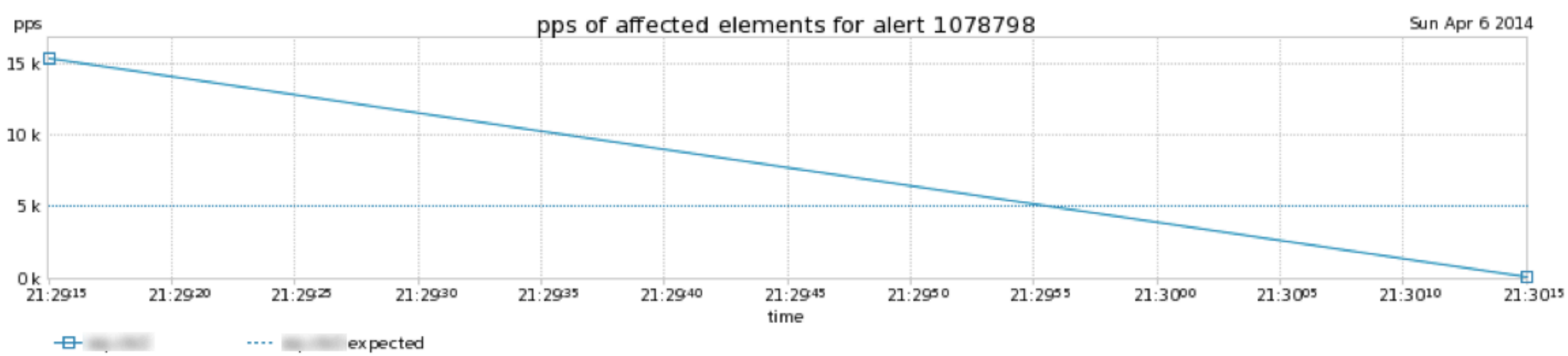
chargen Reflection/Amplification Attack – UDP/19

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



chargen Reflection/Amplification Attack – UDP/19

Affected Network Elements

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

Change Timeframe

Timeframe:

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

Traffic Details for router [illegible]

Summary

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

chargen Reflection/Amplification Attack – UDP/19

Affected Network Elements

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

Change Timeframe

Timeframe:

Other | 2014-04-06 21:29:15 | 2014-04-06 21:30:15 | ↺ | Update

Interval | *Start* | *End*

Traffic Details for router

Summary

	Bytes	Pack[illegible]ts	Bytes/Pkt	bps	pps
	1.11 G	931.0[illegible] k	1.19 k	7[illegible].92 M	7.76 k

chargen Reflection/Amplification Attack – 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
[illegible]/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	☑

chargen Reflection/Amplification Attack – 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
[illegible]/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	☑

chargen Reflection/Amplification Attack – 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	☑

chargen Reflection/Amplification Attack – 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[illegible]/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	☑

chargen Reflection/Amplification Attack – 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 [illegible]	518	572.30 M	488.00 k	1.17 k	38.15 M	4.07 k	52.42	☑
xe-5/1/0.106 [illegible]	521	376.97 M	308.00 k	1.22 k	25.13 M	2.57 k	33.08	☑
xe-4/0/0.104 [illegible]	584	155.73 M	132.00 k	1.18 k	10.38 M	1.10 k	14.18	☑
xe-4/0/1.386 [illegible]	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 [illegible]	519	1.11 G	931.00 k	1.19 k	73.92 M	7.76 k	100.00	☑

SSDP Reflection/Amplification

Amplification Factor - SSDP

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

Characteristics of an SSDP Reflection/Amplification Attack

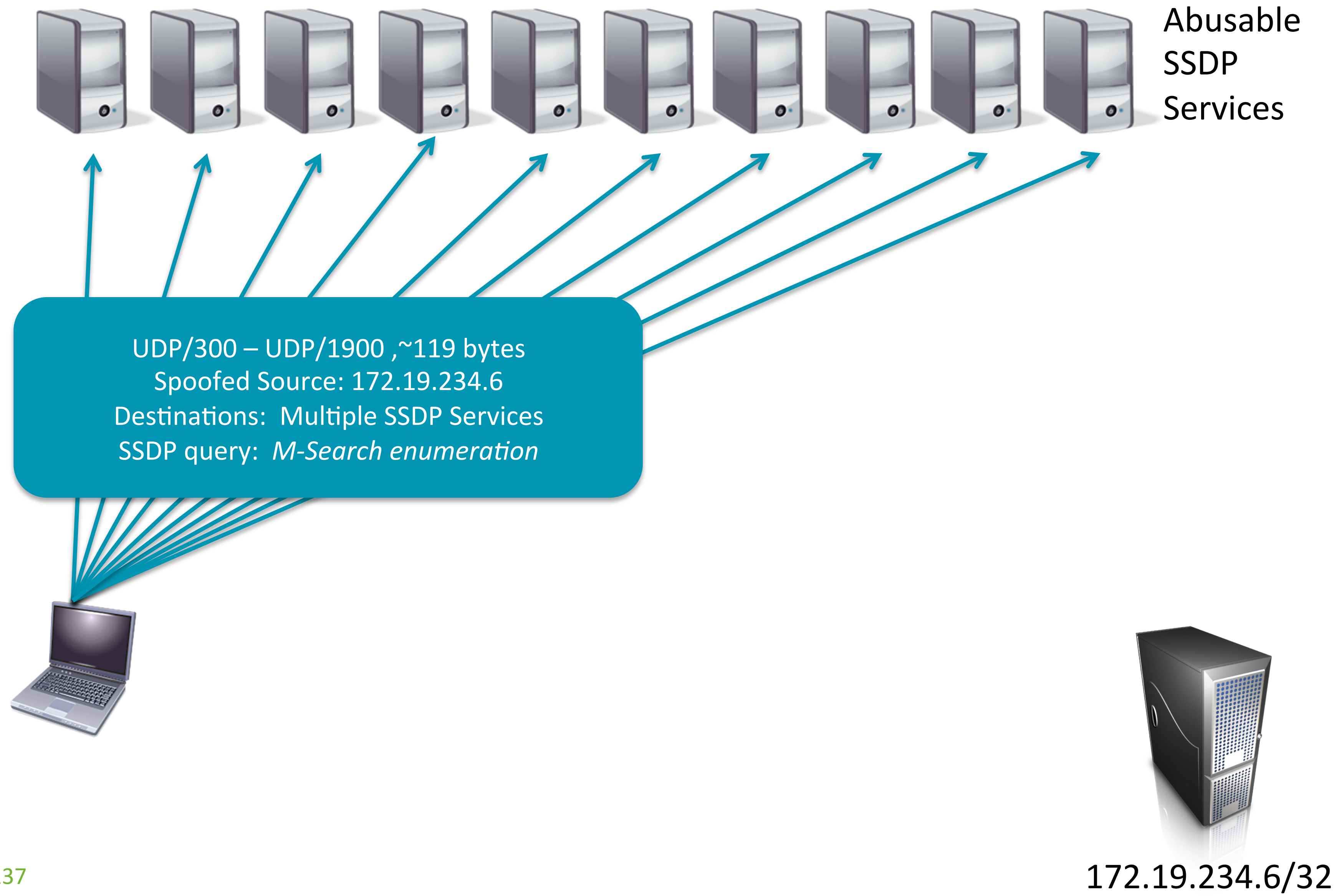
- The attacker spoofs the IP address of the target of the attack, sends an SSDP *M-Search* query to abusable SSDP services running on home CPE devices and some older Windows XP systems These packets are typically ~118 bytes in length.
- The attacker chooses the UDP port which he'd like to target – it can be any port of the attacker's choice – and uses that as the source port. The destination port is UDP/1900.
- The SSDP services 'reply' to the attack target with streams of 1360-byte – 9800-byte packets sourced from UDP/1900; the destination port is the source port the attacker chose when generating the SSDP queries. These packets will consist of initial and non-initial UDP fragments.

Characteristics of an SSDP Reflection/Amplification Attack (cont.)

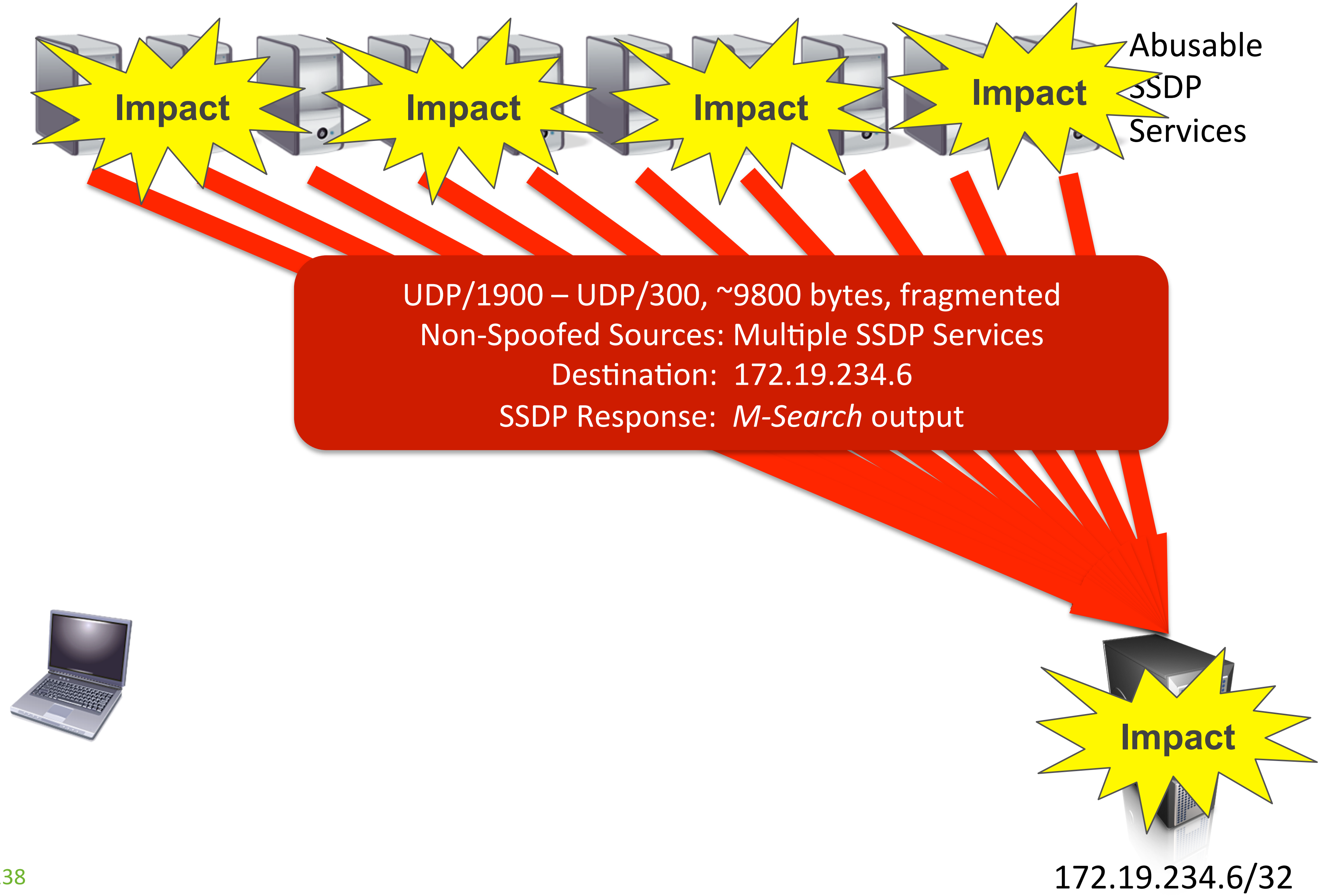
- As these multiple streams of SSDP replies converge, the attack volume can be very large – the largest verified attack of this type so far is over 42gb/sec. 10-35gb/sec attacks are commonplace.
- Due to sheer attack volume, the Internet transit bandwidth of the target, along with core bandwidth of the target's peers/upstreams, as well as the core bandwidth of intermediary networks between the various SSDP services being abused and the target, are saturated.
- More savvy attackers will identify the individual SSDP services available on the abusable SSDP-enabled devices, and enumerate them with iterative parallel spoofed SSDP queries. Lots of non-initial fragments in this scenario, a la DNS.
- In most attacks, between ~4,000-6,000 abusable SSDP services are leveraged by attackers. Up to 10,000 abusable SSDP services have been observed in some attacks.

SSDP Reflection/Amplification Attack Methodology

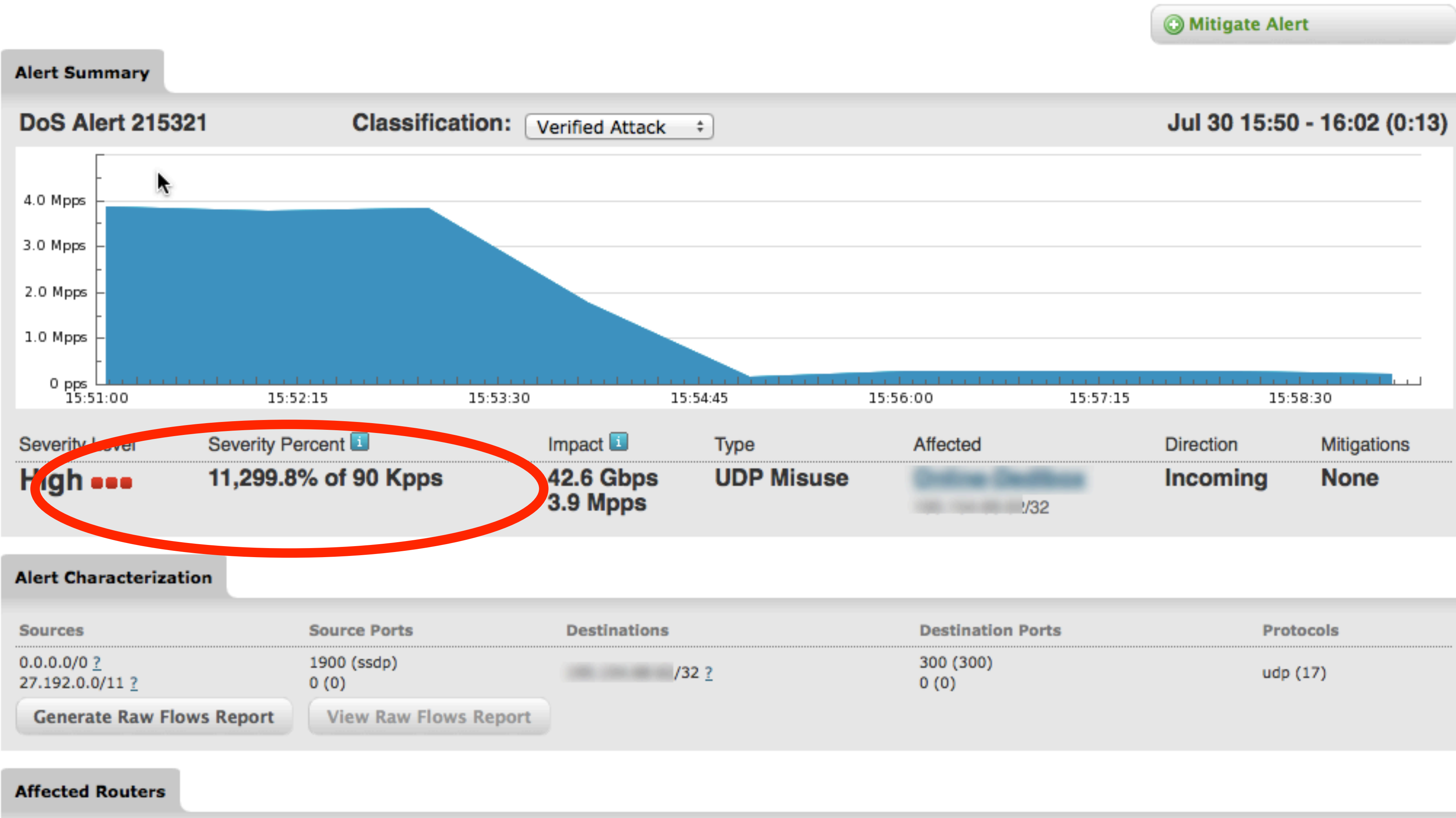
SSDP Reflection/Amplification Attack Methodology



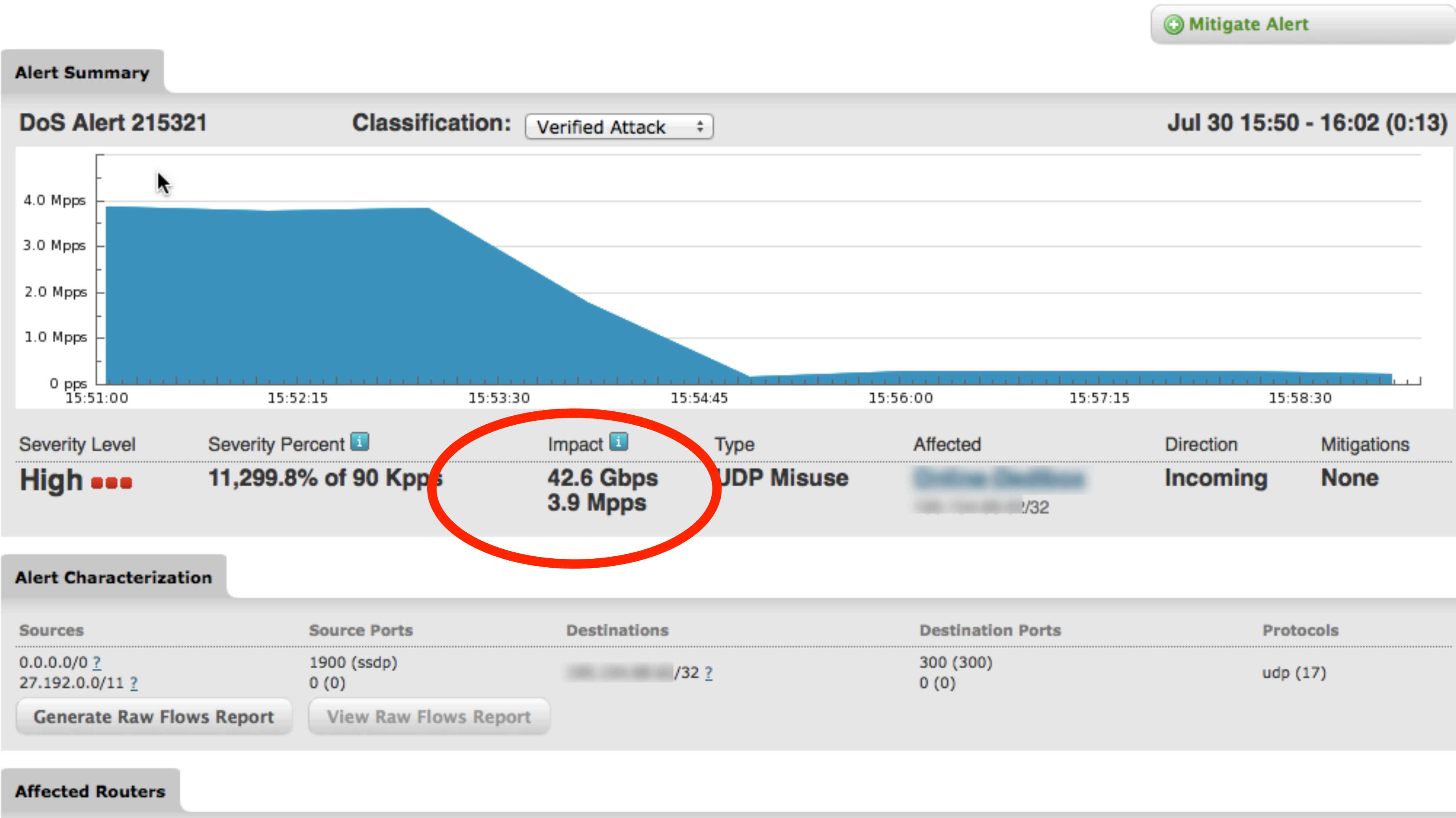
SSDP Reflection/Amplification Attack Methodology



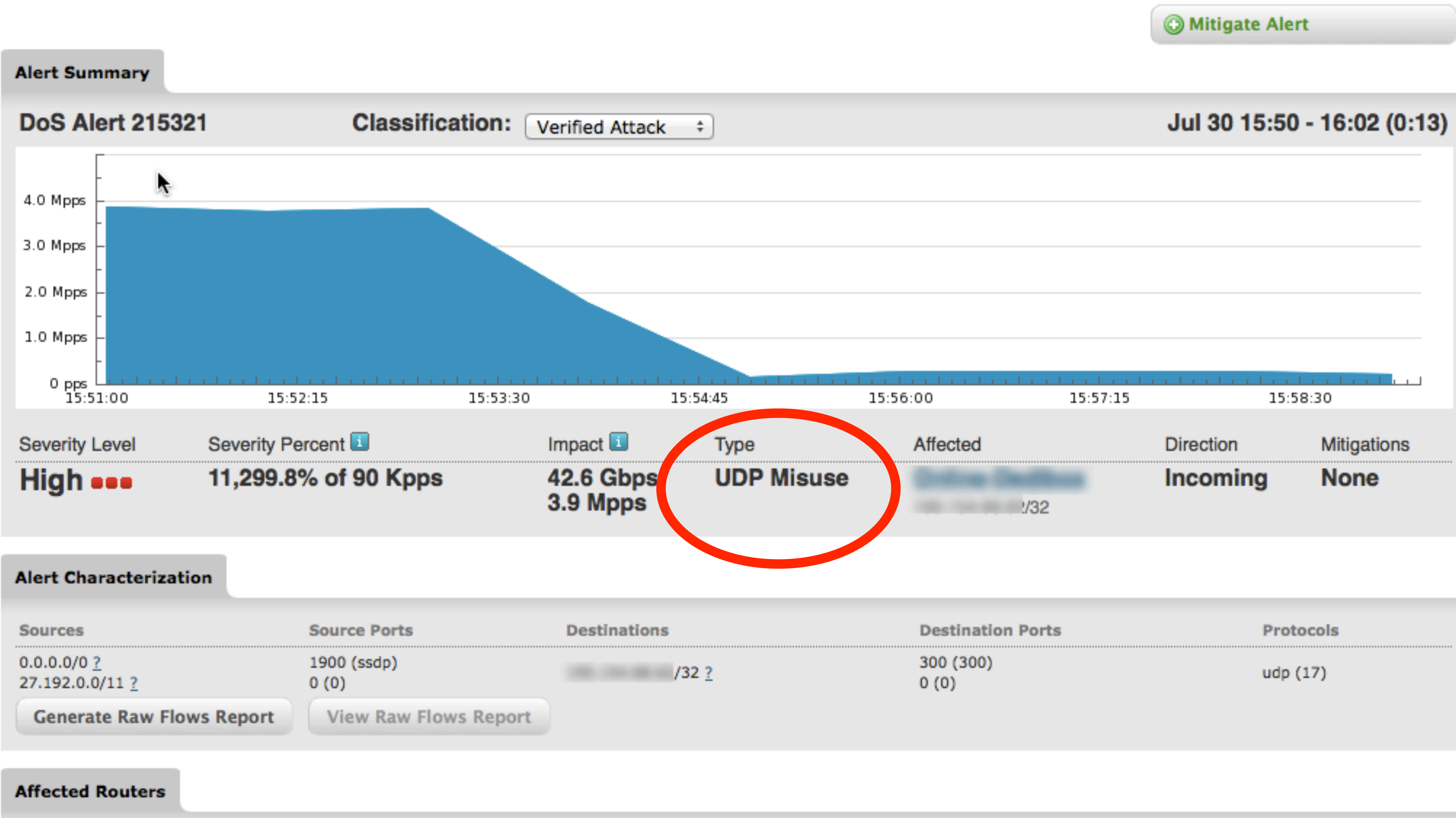
SSDP Reflection/Amplification Attack



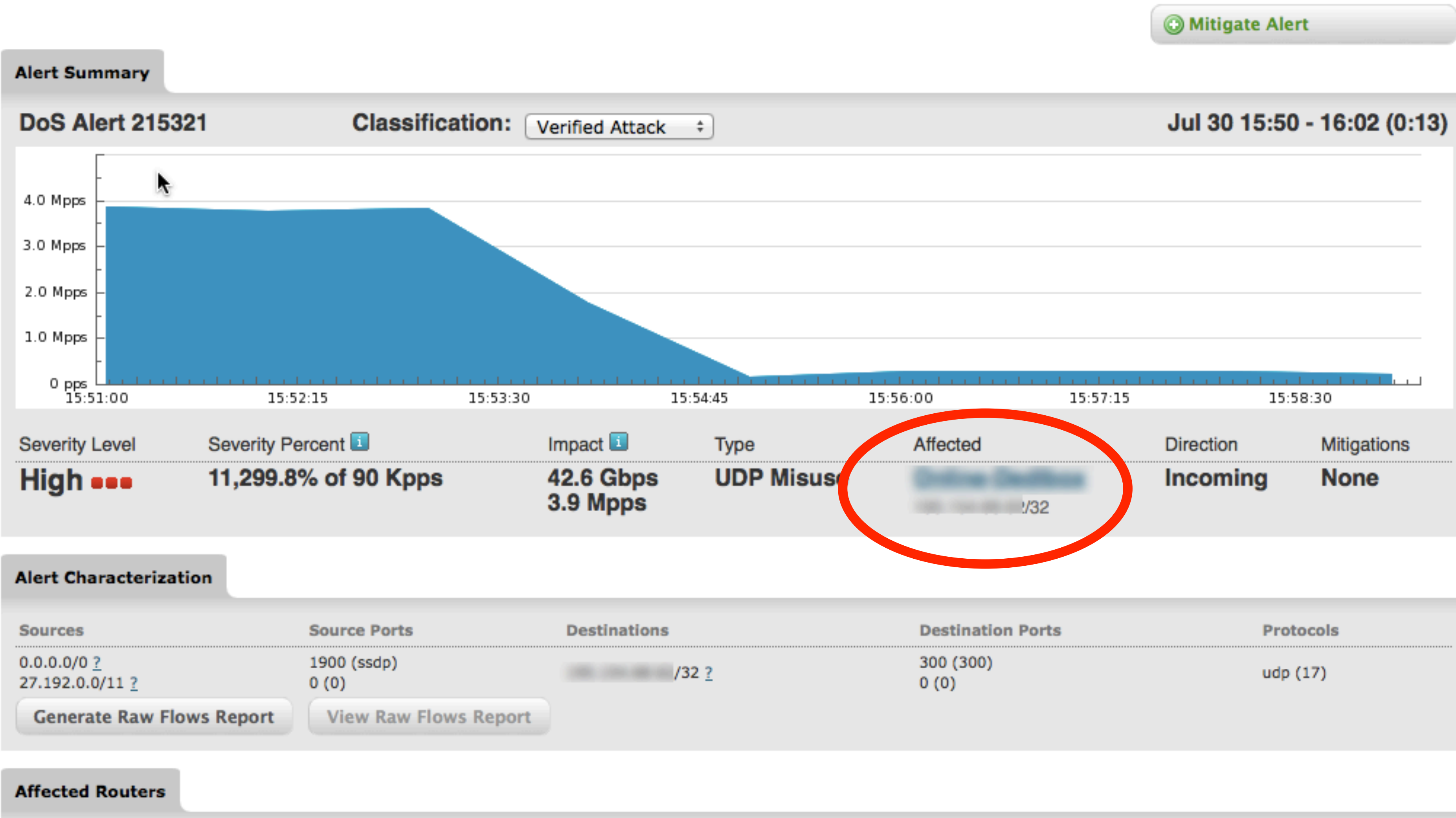
SSDP Reflection/Amplification Attack



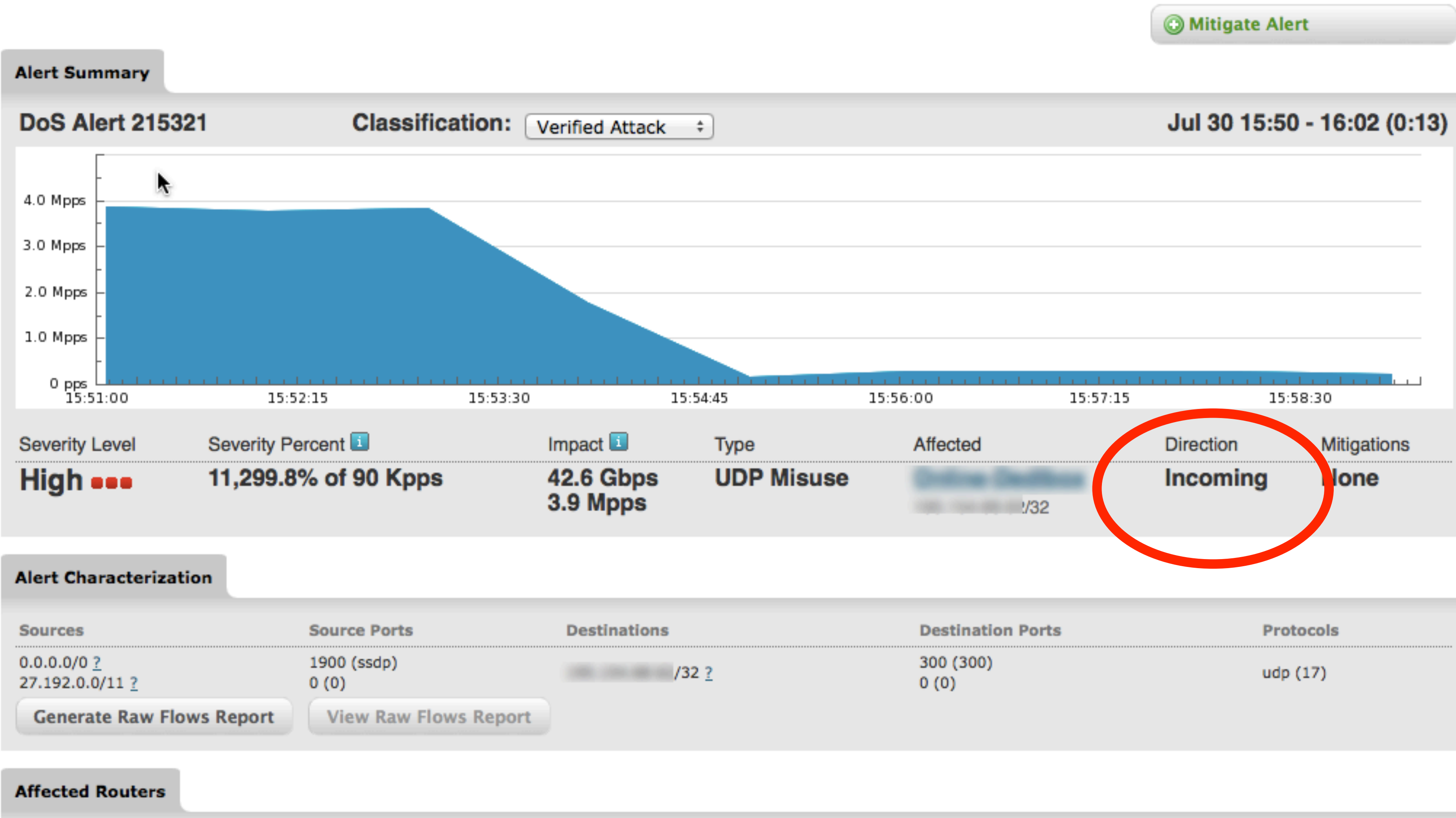
SSDP Reflection/Amplification Attack



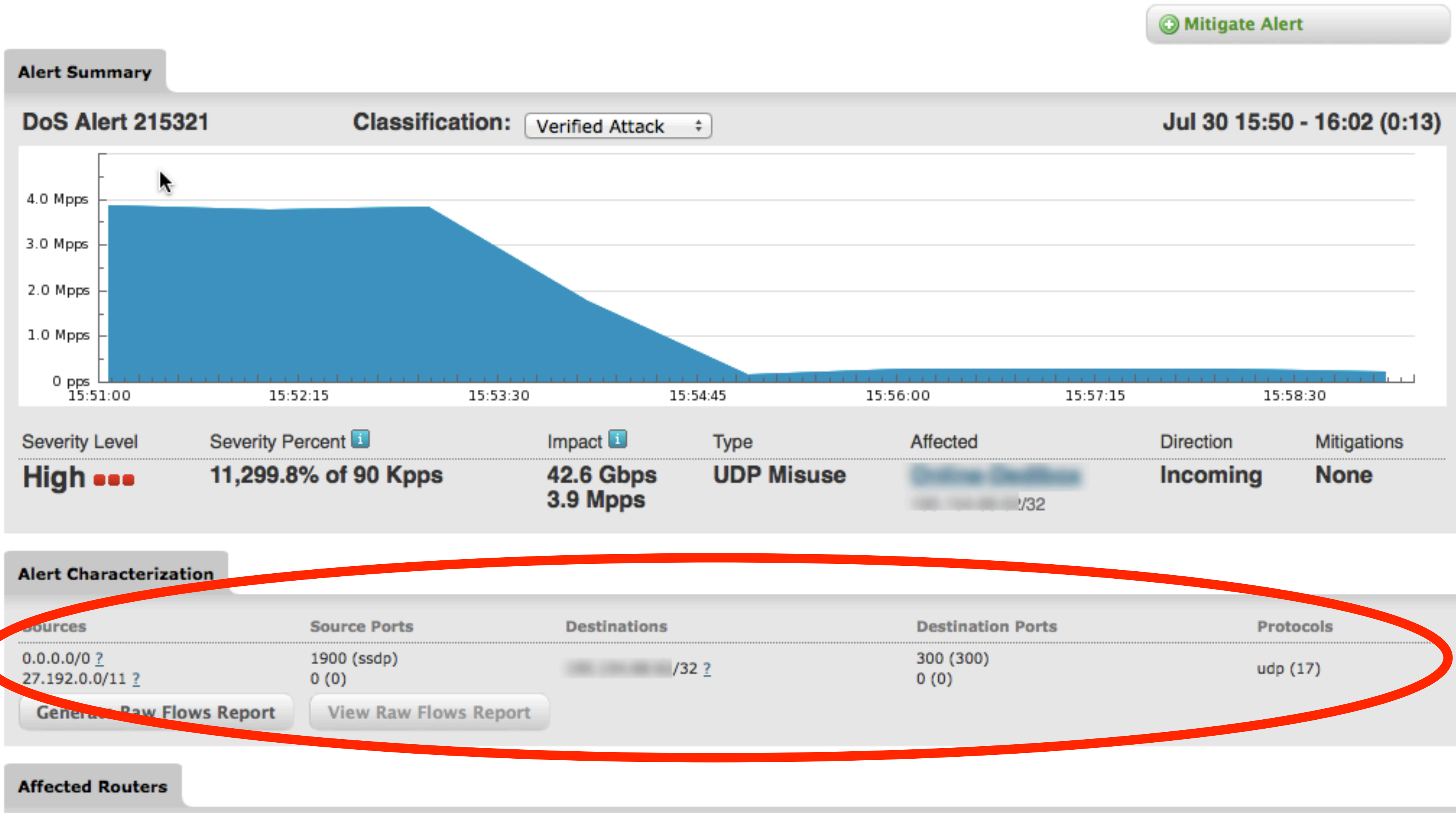
SSDP Reflection/Amplification Attack



SSDP Reflection/Amplification Attack



SSDP Reflection/Amplification Attack



SSDP Reflection/Amplification Attack

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

SSDP Reflection/Amplification Attack

Affected Routers

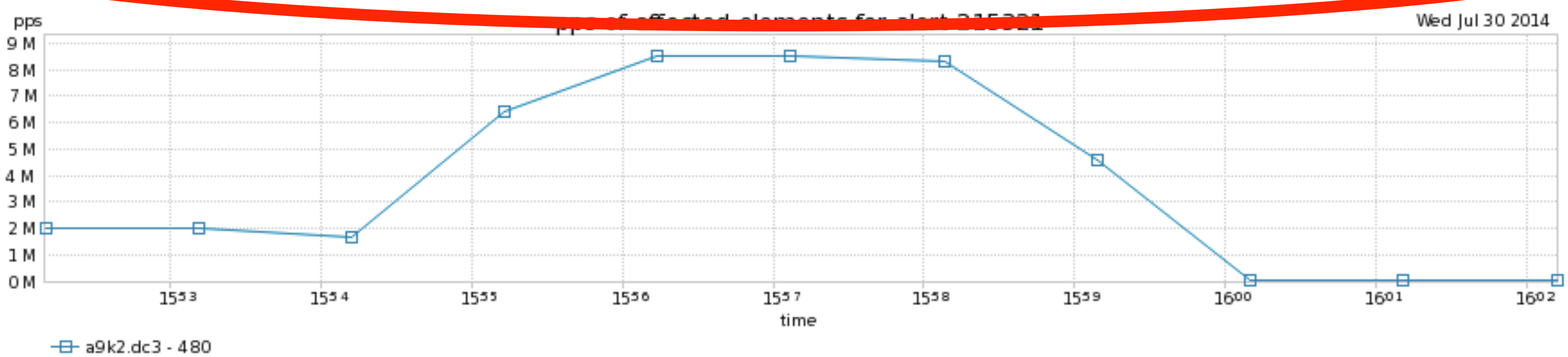
	Severity Level	Expected	Observed bps Max	Observed bps Overall	Observed pps Max	Observed pps Overall	Details
Router	High	50.00 Kpps	40.14 Gbps	20.25 Gbps	9.94 Mpps	4.7[illegible] Mpps	Details
Interface (SNMP 315) Bundle-Ether2.1013		-	1.20 Gbps	549.60 Mbps	287.47 Kpps	166.81 Kp[illegible]	Details
Interface (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) TenGigE0/0/0/11.4080		-	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

SSDP Reflection/Amplification Attack

Mitigate Alert

Alert Summary

ID	Importance	Impact	Duration	Start Time	Direction	Type	Resource
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)	



Affected Network Elements

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

SSDP Reflection/Amplification Attack

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
[illegible]/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

SSDP Reflection/Amplification Attack

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
[illegible]/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

SSDP Reflection/Amplification Attack

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	8.5[illegible] 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

SSDP Reflection/Amplification Attack

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	☐

SSDP Reflection/Amplification Attack

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 [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	☐

How Much Spoofed Traffic Yields a 100gb/sec DDoS Attack?

How Much Spoofed Traffic Yields a 100gb/sec DDoS Attack?

- **DNS - 160:1 amplification factor**
  - **625mb/sec** of spoofed DNS queries for **100gb/sec** attack
  - Largest observed in 2014 – 104gb/sec, 125gb/sec reported

- **ntp - 1000:1 amplification factor**
  - **100mb/sec** of spoofed ntp queries for **100gb/sec** attack
  - Largest observed in 2014 – 325gb/sec, 450gb/sec reported

- **chargen – 18:1 / 1000:1 amplification factor**
  - **100mb/sec - 5.5gb/sec** of spoofed chargen queries for **100gb/sec** attack
  - Largest observed in 2014 – 96gb/sec, 120gb/sec reported

- **SNMP - 880:1 amplification factor for optimized attack**
  - **114mb/sec** of spoofed, iterated SNMP queries for **100gb/sec** attack
  - Largest observed in 2014 – 18gb/sec, 60gb/sec reported

- **SSDP – 20:1 / 83:1 amplification factor**
  - **1.2gb/sec - 5gb/sec** of spoofed SSDP queries for **100gb/sec** attack
  - Largest observed in 2014 – 131gb/sec

- **MS SQL Replication Service, aka SQL Slammer-on-Demand - 173:1 - 473:1 amplification factor**
  - **211mb/sec - 578mb/sec** of spoofed MS SQL RS queries for **100gb/sec** attack
  - Largest observed in 2014 – N/A

Mitigating Reflection/Amplification DDoS Attacks

What *Not* to Do!

- ***Do not*** indiscriminately block UDP/123 on your networks!
- ***Do not*** indiscriminately block UDP/53 on your networks!
- ***Do not*** block UDP/53 packets larger than 512 bytes!
- ***Do not*** block TCP/53 on your networks!
- ***Do not*** indiscriminately block UDP/161 on your networks!
- ***Do not*** indiscriminately block UDP/19 on your networks!
- ***Do not*** indiscriminately block UDP/1900 on your networks!
- ***Do not*** indiscriminately block fragments on your networks!
- ***Do not*** block all ICMP on your networks! At the very least, allow ICMP Type-3/Code-4, required for PMTU-D.

If you do these things, you will ***break the Internet*** for your customers/users!

Don't Be Part of the Problem!

- Deploy **antispoofing** at ***all*** network edges.
  - **uRPF Loose-Mode/Feasible-Mode** at the peering edge
  - **uRPF Strict Mode** at customer aggregation edge
  - **ACLs** at the customer aggregation edge
  - **uRPF Strict-Mode** and/or **ACLs** at the Internet Data Center (IDC) aggregation edge
  - **DHCP Snooping** (works for static addresses, too) and **IP Source Verify** at the IDC LAN access edge
  - **PACLs** & **VACLs** at the IDC LAN access edge
  - **Cable IP Source Verify**, etc. at the CMTS
  - **Other** DOCSIS & DSL mechanisms
- If you get a reputation as a spoofing-friendly network, you will be **de-peered/de-transited** and/or **blocked**!

Don't Be Part of the Problem! (cont.)

- ***Proactively scan*** for and remediate abusable services ***on your network*** and on ***customer/user networks***, including blocking traffic to/from abusable services if necessary in order to attain compliance
- Check http://www.openntpproject.org to see if abusable NTP services have been identified on your networks and/or customer/user networks
- Check http://www.openresolverproject.org to see if abusable open DNS recursors have been identified on your network or on customer/user networks.
- ***Collateral damage*** from these attacks is widespread – if there are abusable services on your networks or customer/user networks***, your customers/users will experience significant outages*** and performance issues, and your help-desk will light up!

Detection/Classification/Traceback/Mitigation

- Utilize **flow telemetry** (NetFlow, cflowd/jflow, etc.) exported from *all* network edges for attack detection/classification/traceback
  - Many open-source tools available, no excuse not to get started!
- Enforce **standard network access policies** in front of servers/ services via stateless ACLs in hardware-based routers/layer-3 switches.
- Ensure recursive DNS servers are **not queryable** from the public Internet – only from your customers/users.
- Ensure **SNMP is disabled/blocked** on public-facing infrastructure/servers.
- Disallow **level-6/-7 NTP queries** from the public Internet.
- Disable all **unnecessary services** such as chargen.
- **Regularly audit** network infrastructure and servers/services.

Detection/Classification/Traceback/Mitigation (cont.)

- Deploy network infrastructure-based reaction/mitigation techniques such as **S/RTBH** and **flowspec** at ***all*** network edges.
- Deploy intelligent DDoS mitigation systems (IDMSes) in mitigation centers located at topologically-appropriate points within your networks to mitigate attacks.
- Ensure ***sufficient mitigation capacity and diversion/re-injection bandwidth*** – S/RTBH, flowspec, IDMS. Consider OOB mitigation center links from edge routers to guarantee 'scrubbing' bandwidth.
- Enterprises/ASPs should subscribe to '**Clean Pipes**' DDoS mitigation services from ISPs/MSSPs.
- Consumer broadband operators should consider **minimal default ACLs** to limit the impact of service abuse on customer networks.
- User the **power of the RFP** to specify secure default configurations for PE & CPE devices – and verify via testing.
- **Know who to contact** at your peers/transits to get help.
- **Participate** in the global operational security community.

Detection/Classification/Traceback/Mitigation (cont.)

- ISPs should consider deploying **Quality-of-Service (QoS)** mechanisms at all network edges to police non-timesync NTP traffic down to an appropriate level (i.e., 1mb/sec).
  - NTP timesync packets are 76 bytes in length (all sizes are minus layer-2 framing)
  - NTP monlist replies are ~468 bytes in length
  - Observed NTP monlist requests utilized in these attacks are 50, 60, and 234 bytes in length
  - **Option 1** – police all non-76-byte UDP/123 traffic (source, destination, or both) down to 1mb/sec. This will police both attack source – reflector/amplifier traffic as well as reflector/amplifier – target traffic
  - **Option 2** – police all 400-byte or larger UDP/123 traffic (source) down to 1mb/sec. This will police only reflector/amplifier – target traffic
  - NTP timesync traffic will be unaffected
  - Additional administrative (rarely-used) NTP functions such as *ntptrace* will only be affected during an attack
- Enterprises/ASPs should only allow NTP queries/responses to/from **specific NTP services**, disallow all others.

Scaling Mitigation Capacity - 4tb/sec and Beyond

- Currently-shipping largest-capacity Intelligent DDoS Mitigation System (IDMS) – 40gb/sec
- 16-IDMS (CEF/ECMP limit) = 640gb/sec per cluster
- Multiple clusters can be anycasted
- Largest number of IDMSes per deployment currently 100 = 4tb/sec of mitigation capacity per deployment, 10x more than largest DDoS to date.
- Deploy IDMSes in mitigation centers at edges - in/out of edge devices.
- Deploy IDMSes in regional or centralized mitigation centers with dedicated, high-capacity OOB diversion/re-injection links. Sufficient bandwidth for diversion/re-injection is key!
- S/RTBH & flowspec leverage router/switch hardware, hundreds of mpps, gb/sec. Leveraging network infrastructure is required due to ratio of attack volumes to peering and core link capacities!

Conclusion

Reflection/Amplification DDoS Attack Summary

- Abusable services are widely misimplemented/ misconfigured across the Internet
- Large pools of abusable servers/services
- Gaps in anti-spoofing at network edges
- High amplification ratios
- Low difficulty of execution
- Readily-available attack tools
- Extremely high impact – ‘The sky is falling!’
- Significant risk for potential targets and intermediate networks/bystanders

On the Origins of Spoofed Traffic

- NAT is ugly, breaks things, and has no inherent security value.
- However, there's been one beneficial side-effect of the prevalence of NAT on broadband access networks – anti-spoofing (you generally can't spoof traffic from behind a NAT, unless it's broken).
- We believe that a lot of the spoofed traffic used to initiate reflection/amplification DDoS attacks originates from servers under the control of attackers in hosting/co-location/VPS/'cloud' Internet Data Centers (IDCs) which don't enforce source address validation.
- Servers may be compromised; may be VPS rented by attackers; may be hosted by 'bulletproof' providers.
- Flow telemetry collection/analysis tools perform automagic traceback of spoofed traffic to network ingress points - but only within one's own span of administrative control.

What is to Be Done?

- Initiate project to rent shell/VPS instances around the world, run Spoofer Project-type code on VPS instances, compile reports of IDCs/hosters/co-locators who allow spoofing. Somewhere to start, at least.

- Discuss the possibility of including Spoofer Project-type functionality in operating systems with the relevant vendors/organizations (Microsoft, Apple, Google, Linux distros, *BSD distros, console vendors, Cisco, Juniper, Linksys, Asus, etc.).

- Learning mechanism for IP Source Guard- or pACL/vACL-type functionality enabled by default on layer-2 switch ports configured as access ports – network infrastructure vendors. IDC access-layer is a relatively restricted domain with a smaller scope for undesirable outcomes and greater probability of success.

- ‘SDN’ auto-provisioning of source address validation mechanisms? >*cringe*<

- Improve spoofed traffic classification, inter-operator cooperative traceback capabilities – flow telemetry collection/analysis tool vendors.

- Work with insurance companies to help them understand unsecured risks, develop auditing capabilities.

Are We Doomed?

- No! Deploying existing, well-known tools/techniques/BCPs results in a vastly improved security posture with measurable results.
- Evolution of defenses against these attacks demonstrates that positive change is possible – targeted organizations & defending ISPs/MSSPs have altered architectures, mitigation techniques, processes, and procedures to successfully mitigate these attacks.
- Mitigation capacities are scaling to meet and exceed attack volumes – deployment architecture, diversion/re-injection bandwidth, leveraging network infrastructure are key.
- Automation is a Good Thing, but it is no substitute for resilient architecture, insightful planning, and smart opsec personnel, who are more important now than ever before!

Discussion

This Presentation – http://bit.ly/1lHksUH

ARBOR NETWORKS

Special thanks to Gary Sockrider & Ben Fischer of Arbor Networks for their contributions to this presentation.

Thank You!

Roland Dobbins <rdobbins@arbor.net>
Senior ASERT Analyst