

# Security Track

NANOG 65

# BGPStream

Nanog65

Andree Toonk

[andree@bgpmon.net](mailto:andree@bgpmon.net)



# BGPStream

## Questions we'd like to answer

*Someone hijacked my Prefix!*

*Now what? Was it targeted? Were others affected as well?*

*I hear rumors about a large outage in \$country / \$ISP*

*Is that true? How large is it? Who's affected?  
What time did it start?*



# BGPStream

1. BGP Hijacks
2. BGP leaks
3. Large scale outages

<https://bgpstream.com/>

<https://twitter.com/bgpstream>



**bgpstream** @bgpstream · Sep 18

BGP,HJ,hijacked prefix AS15169  
1.1.1.0/24, Google Inc.,-,By AS9950  
DACOM, [bgpstream.com/event/1058](https://bgpstream.com/event/1058)



25



10



# BGPStream – BGP Hijack

## Possible BGP hijack

Beginning at 2015-09-30 02:56:39, we detected a possible BGP hijack.

Prefix 54.210.0.0/16, Normally announced by AS14618 Amazon.com, Inc.

Starting at 2015-09-30 02:56:39, a more specific route (54.210.90.0/24) was announced by ASN 9299.

This was detected by 72 BGPMon peers.

---

### Expected

---

Start time: 2015-09-30 02:56:39

---

Expected prefix: 54.210.0.0/16

---

Expected ASN: 14618  (Amazon.com, Inc.)

---

### Event Details

---

Detected advertisement: 54.210.90.0/24

---

Detected Origin ASN 9299  (Philippine Long Distance Telephone Company)

---

Detected AS Path 58786 9957 38091 9848 15412 3257 2914 9299

---

Detected by number of BGPMon peers: 72

# BGPStream – Outages

[BGPStream](#)[About](#)[Contact](#)

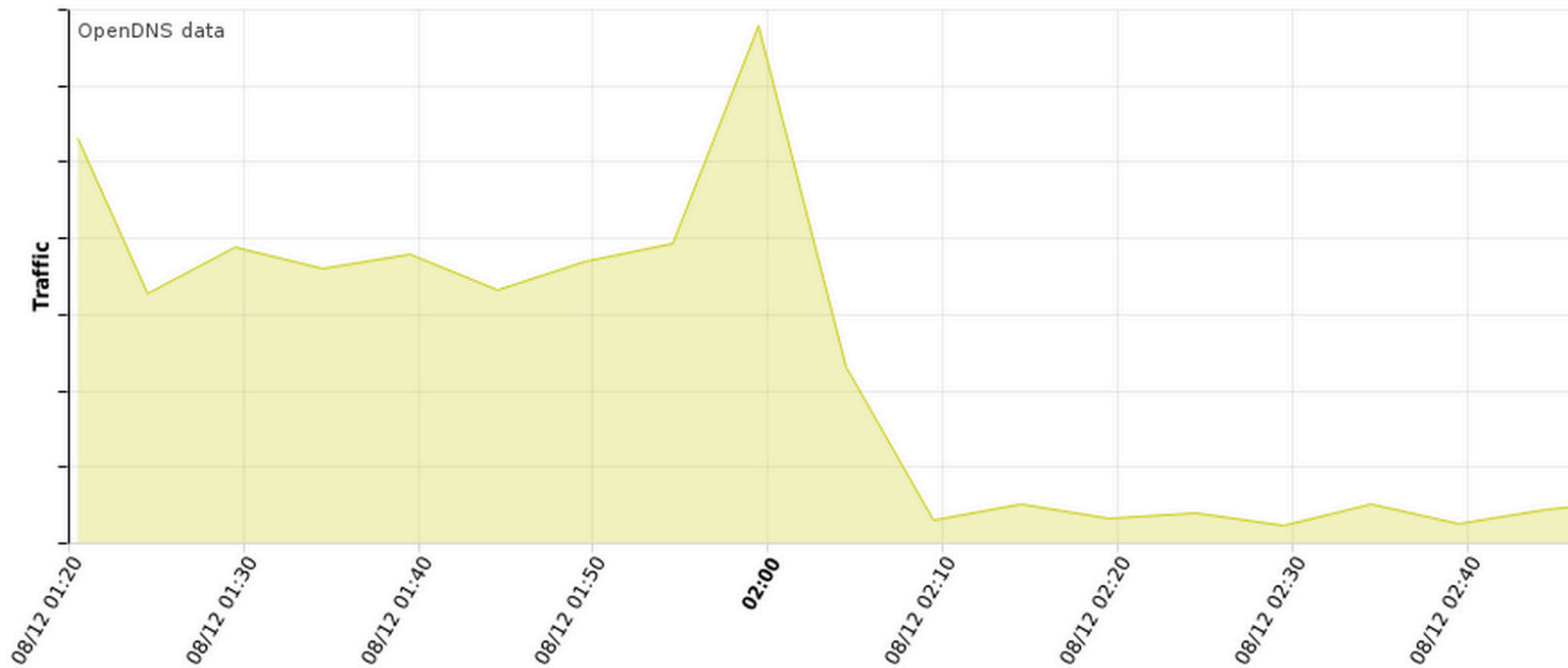
Beginning at 2015-08-12 02:05:00, we detected an outage for Iraq 🇮🇶

Start time: 2015-08-12 02:05:00

Number of Prefixes Affected: 237 (39%)

Previous two hours traffic from Iraq

## OpenDNS Traffic from Country (IQ)



# BGPStream – BGP leaks

## BGP Leak

Beginning at 2015-10-05 15:29:38, we detected a possible BGP Leak

Prefix 162.158.22.0/24, Normally announced by AS13335 CloudFlare, Inc.

Leaked by AS8781 Ooredoo Q.S.C.

This was detected by 6 BGPMon peers.

---

### Leak Details

---

Start time: 2015-10-05 15:29:38

---

Leaked prefix: 162.158.22.0/24 (AS13335 CloudFlare, Inc.)

---

Leaked By: AS8781  (Ooredoo Q.S.C.)

---

Leaked To:

- 15412 (Flag Telecom Global Internet AS)

---

Example AS path: 48284 8881 2914 15412 8781 1299 13335

---

Number of BGPMon peers that saw it: 6

## Watch the replay of this event

# Detecting hijacks

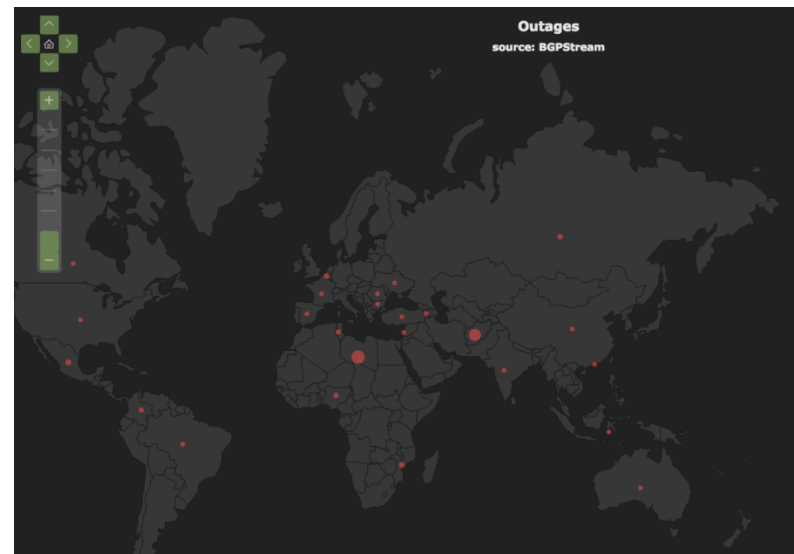
# MONITOR



- Existing Business relationship?
  - Does the Detected AS announce other Expected AS prefixes in BGP
  - Is there an existing peering relationship
  - Did Detected AS recently announce Expected AS prefixes
  - Exclude well known relations and ASNs (i.e. DoD Asns, special Anycast prefixes).
- Whois information
  - Valid RPLS route object in RIR / IRR databases?
  - Allocation data
  - Name collision in name, description, emails, prefix desc,, AS name
- Geo Info
  - Do Expected and Detected operate in same country
  - For US, same state
  - Detected by number of BGPmon peers



# Questions



Email: [andree@bgpmon.net](mailto:andree@bgpmon.net)  
<https://bgpstream.com>

Twitter: [@bgpstream](https://twitter.com/bgpstream)  
Twitter: [@bgpmon](https://twitter.com/bgpmon)  
Twitter: [@atoonk](https://twitter.com/atoonk)



# Questions



- [Email: andree@bgpmon.net](mailto:andree@bgpmon.net)
- [Twitter: @bgpstream](https://twitter.com/bgpstream)
- [Twitter: @bgpmon](https://twitter.com/bgpmon)
- [Twitter: @atoonk](https://twitter.com/atoonk)



# **New IRR Tools**

Job Snijders

job@ntt.net

# What is the IRR?

- A collection of independently operated database instances which store text objects
- End-users submit data to the IRR, carriers retrieve that data from the IRR.
- NTT recognizes the following: **AFRINIC**, BBOI, TC, ALTDB, **APNIC**, ARIN, BELL, GT, JPIRR, LEVEL3, RADB, RGNET, **RIPE**, SAVVIS
- Different IRRs have different rules

# Quality differences

- Coupling between RIR & IRR functionality?
  - Does the IP owner have to authorize route object creation?
- Verification queuing?
- Yearly payment as keep-alive?
- 24/7 support staff?
- Easily accessible training?
- ....

# What makes RIPE's database open source software special?

- NTT can trust the authentication chain from IP block owner ("*inetnum owner*") down to route object creation: both aut-num owner and inetnum owner have to approve

(APNIC & AfriNIC also offer this style of authorization!)

# IRR Homing Recommendation

Knowing that RIPE administrates a decent registry, we encourage everyone with RIPE space to register the route-objects in the RIPE IRR.

RIPE space -> RIPE IRR

APNIC space -> APNIC IRR

Etc etc....

# IRR EXPLORER



New IRR tools - NANOG65 - [job@ntt.net](mailto:job@ntt.net)



# Why IRR Explorer?

- Get a sense of where people registered route-objects covering your own space
- Motivate people to clean up! 😊
- I grew tired of

```
$ peval | awk | sed | derp | help | echo "get  
me out of here" | wall -g
```

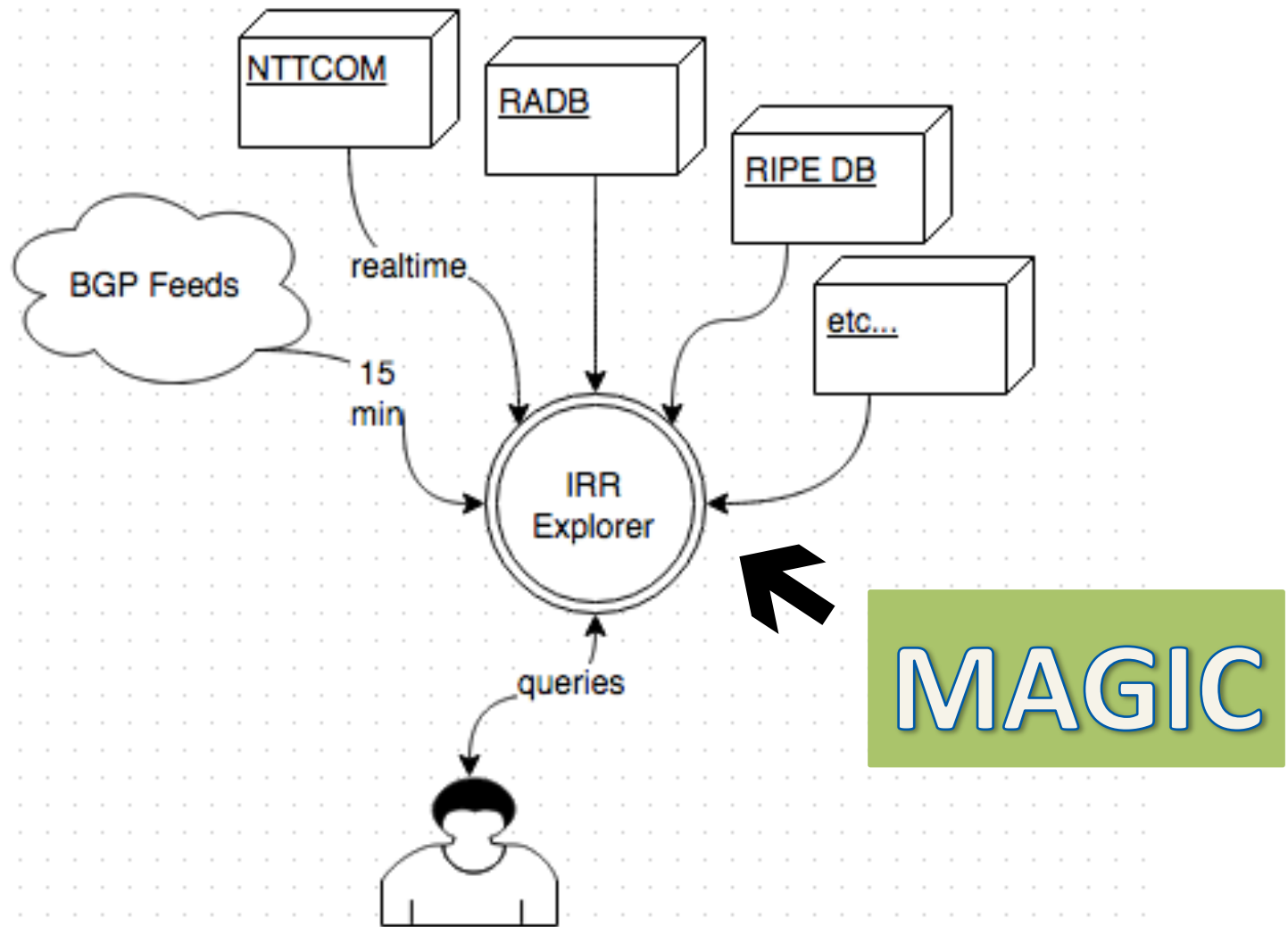
# Debugging your IRR data

## IRR Explorer

<http://irrexplorer.nlnog.net/> is a tool to search where your IRR objects are located and see if they are in the proper database or not

Code: <https://github.com/job/irrexplorer>

# IRR explorer overview





Enter an IP address, prefix, AS Number, or  
AS-SET

Submit



217.170.0.19

Search

## Prefix: 217.170.0.19

### Matching prefixes

prefix	bgp	ripe_managed	ripe	nttcom	bboi	advice
217.170.11.0/24	24785	✓		24785		Prefix is in DFZ and has an IRR record, but NOT in RIPE! BGP origin matches IRR entries.
217.170.20.0/24	24785	✓				Prefix is in DFZ, but NOT registered in any IRR and should go into RIPE!
217.170.22.0/24	24785	✓				Prefix is in DFZ, but NOT registered in any IRR and should go into RIPE!
217.170.22.0/25	24785	✓				Prefix is in DFZ, but NOT registered in any IRR and should go into RIPE!
217.170.23.0/24	24785	✓				Prefix is in DFZ, but NOT registered in any IRR and should go into RIPE!
217.170.15.0/24	5418	✓	5418			Perfect
217.170.4.0/22	16243	✓	16243			Perfect
217.170.0.0/19		✓	24785			Not seen in BGP, but (legacy?) route-objects exist, consider clean-up
217.170.0.0/20		✓	24785			Not seen in BGP, but (legacy?) route-objects exist, consider clean-up




Search

## AS Number: 15562

### Prefixes

prefix	bgp	ripe_managed	ripe	nttcom	altdb	arin	advice
2001:728::/32	2914	✓		2914			Prefix is in DFZ and has an IRR record, but NOT in RIPE! BGP origin matches IRR entries.
128.242.137.0/24	15562						Prefix in DFZ, but no route-object with correct origin anywhere
194.33.96.0/24	15562	✓	15562				Perfect
2001:67c:208c::/48	15562	✓	15562			15562	Perfect
2001:67c:2980::/48	15562	✓	15562				Perfect
128.242.128.0/22				15562			Not seen in BGP, but (legacy?) route-objects exist, consider clean-up
128.242.132.0/22				15562			Not seen in BGP, but (legacy?) route-objects exist, consider clean-up
128.242.136.0/21				15562			Not seen in BGP, but (legacy?) route-objects exist, consider clean-up



irrexplorer.nlnog.net/search/194.33.96.0/24



Search

Prefix: 194.33.96.0/24

Matching prefixes

prefix	bgp	ripe_managed	ripe	advice
194.33.96.0/24	15562	✓	15562	Perfect

Showing 1 to 1 of 1 entries

# Next tool!

**Irrtree** – *a simple tool to quickly assess potential resource consumption of an AS-SET.*

Homepage: <https://github.com/job/irrtree>

Python install: `pip install irrtree`

No logo



# Example AS-SET

```
$ whois -h rr.ntt.net AS2914:AS-GLOBAL
as-set:      AS2914:AS-GLOBAL
descr:       NTT Communications Global IP
Network transit customers
members:      AS2914, AS3949,
              AS2914:AS-US,
              AS2914:AS-ASIA,
              AS2914:AS-EUROPE,
              AS2914:AS-SA,
              AS2914:AS-OCEANIA
admin-c:      NCGE-VRIO
tech-c:       NCGE-VRIO
```

# Why do we need irrtree?!

How many times did you have bgpq3 or irrtoolset, irrpt or any other filter generator blow up because a customer added crazy AS-SETS to their own?

If someone adds AS2914:AS-GLOBAL to their own AS-SET, the resulting prefix-filter will include ~ **300,000** extra lines

**\$ irrtree AS-COLOCLUE**

IRRTree (1.1.0) report for 'AS-COLOCLUE' (IPv4), using rr.ntt.net at 2015-10-06 10:20

AS-COLOCLUE (6 ASNs, 80 pfxs)

+-- AS-STEFFANN-IPv4 (3 ASNs, 9 pfxs)

| +-- AS15562 (8 pfxs)

| +-- AS57771 (1 pfxs)

| +-- AS203993 (0 pfxs)

+-- AS-SNIJDERS (2 ASNs, 9 pfxs)

| +-- AS-ESGOB-ANYCAST (1 ASNs, 1 pfxs)

| | +-- AS60564 (1 pfxs)

| +-- AS15562 (8 pfxs)

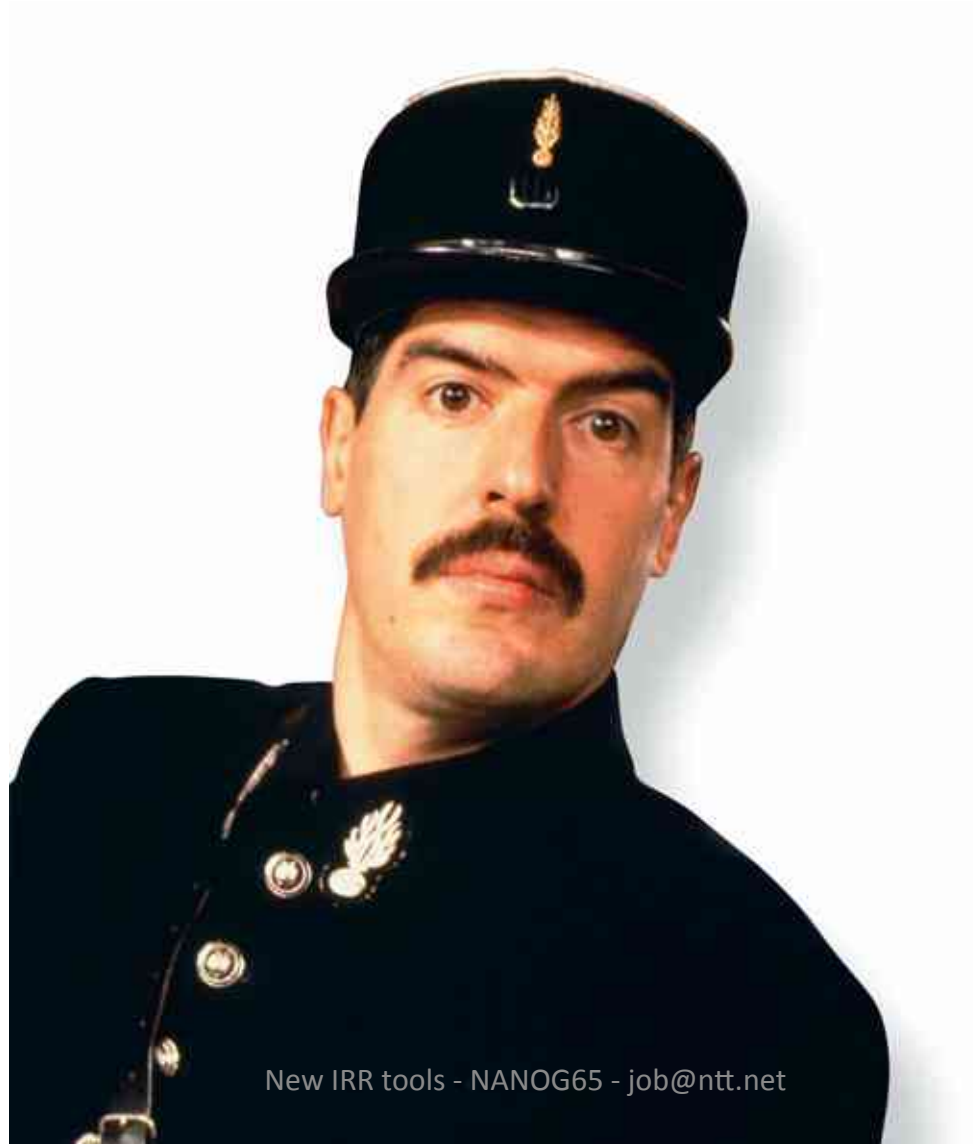
+-- AS47065 (65 pfxs)

+-- AS8283 (5 pfxs)

```
$ irrtree -s AS15562 AS2914:AS-EUROPE  
IRRTree (1.0.0) report for 'AS2914:AS-  
EUROPE' (IPv4), using rr.ntt.net at  
2015-07-07 23:02
```

```
AS2914:AS-EUROPE (30098 ASNs)  
  +-- AS-SERVERCENTRAL (116 ASNs)  
    |   +-- AS-SERVERCENTRAL-CUSTOMERS (115  
ASNs)  
    |       +-- AS-YOUR-GLOBAL-SET (6 ASNs)  
    |           +-- AS-YOUR-CUSTOMERS (4  
ASNs)  
    |               +-- AS15562 (8 pfxs)  
  +-- AS-EASYNET (365 ASNs)  
    |   +-- AS-EASYNETNL (28 ASNs)  
    |       +-- AS-CONCEPTS (3 ASNs) —  
already
```

# Q&A for the routing police



New IRR tools - NANOG65 - [job@ntt.net](mailto:job@ntt.net)

# BGPuma: Are You Being Route Hijacked?

Leigh Metcalf, lbmetcalf@cert.org  
NANOG

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT® is a registered mark of Carnegie Mellon University.

DM-0002832

# BGPuma

- Border Gateway Protocol Update Metric Analysis
- Software that finds route announcements that affect a given list of CIDR blocks.
- We look for subnets and supernets of the given CIDR
  - $\text{CIDR}_1 \subseteq \text{CIDR} \subseteq \text{CIDR}_2$



# Route Injections – What are they good for?

- Presentation at NANOG 60 in Atlanta
- In Summary:
- I found IP addresses related to domains that were related to malware, where the IP addresses were found in Route Injections

# Route Injections

- So we know they exist and we know they can be bad...
- And you can use bgpuma to see if they affect you.

# BGPuma Example

- CERT blog post on cache poisoning:
- <https://insights.sei.cmu.edu/cert/2014/09/-probable-cache-poisoning-of-mail-handling-domains.html>
- Jonathan Spring and I put this up last year. I was asked if it was still occurring and during my research wondered...
- ...are there any route injections affecting the mail handling domains?

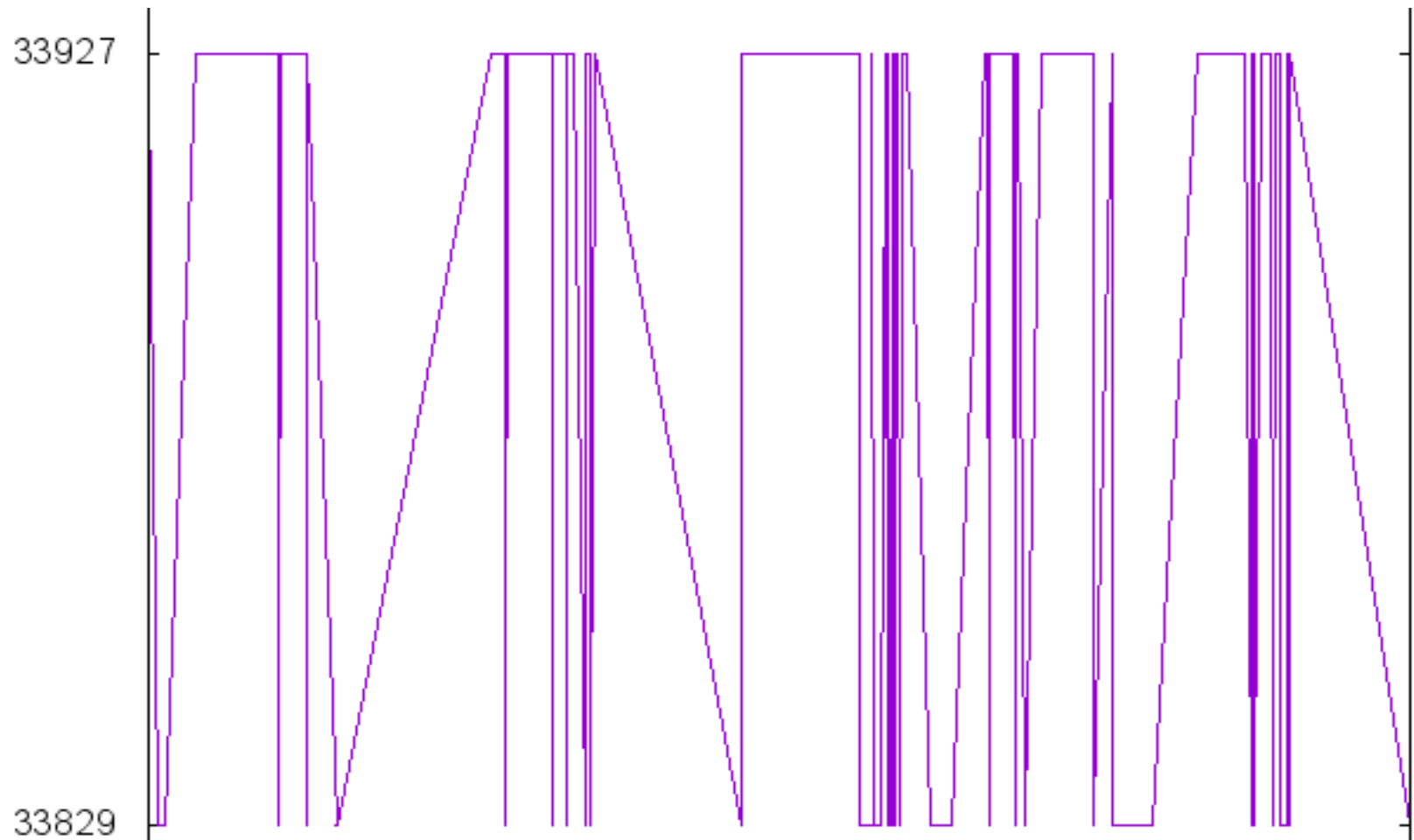
# BGPuma example

- I knew Google was affected in the first results. So I made a list of four IP ranges that were owned by Google: 8.8.8.0/24, 74.125.0.0/16, 64.233.160.0/19, 173.194.0.0/16
- I found instances of a Russian AS announcing 74.125.139.132/32
- Level3, Postini and Google also showed up as announcing the CIDR blocks.

# BGPuma Example #2

- I also study route flapping (this data is available on <http://routeviews-mirror.cert.org>)
- I took one day and found a CIDR block that was flapping... so I took that block and fed it to BGPuma for the day.
- 33927 owned the netblock, 33829 kept announcing it as well.

# BGPuma Example #2



Questions/comments?



# Prevent BGP route-leaks and hijacks before they happen

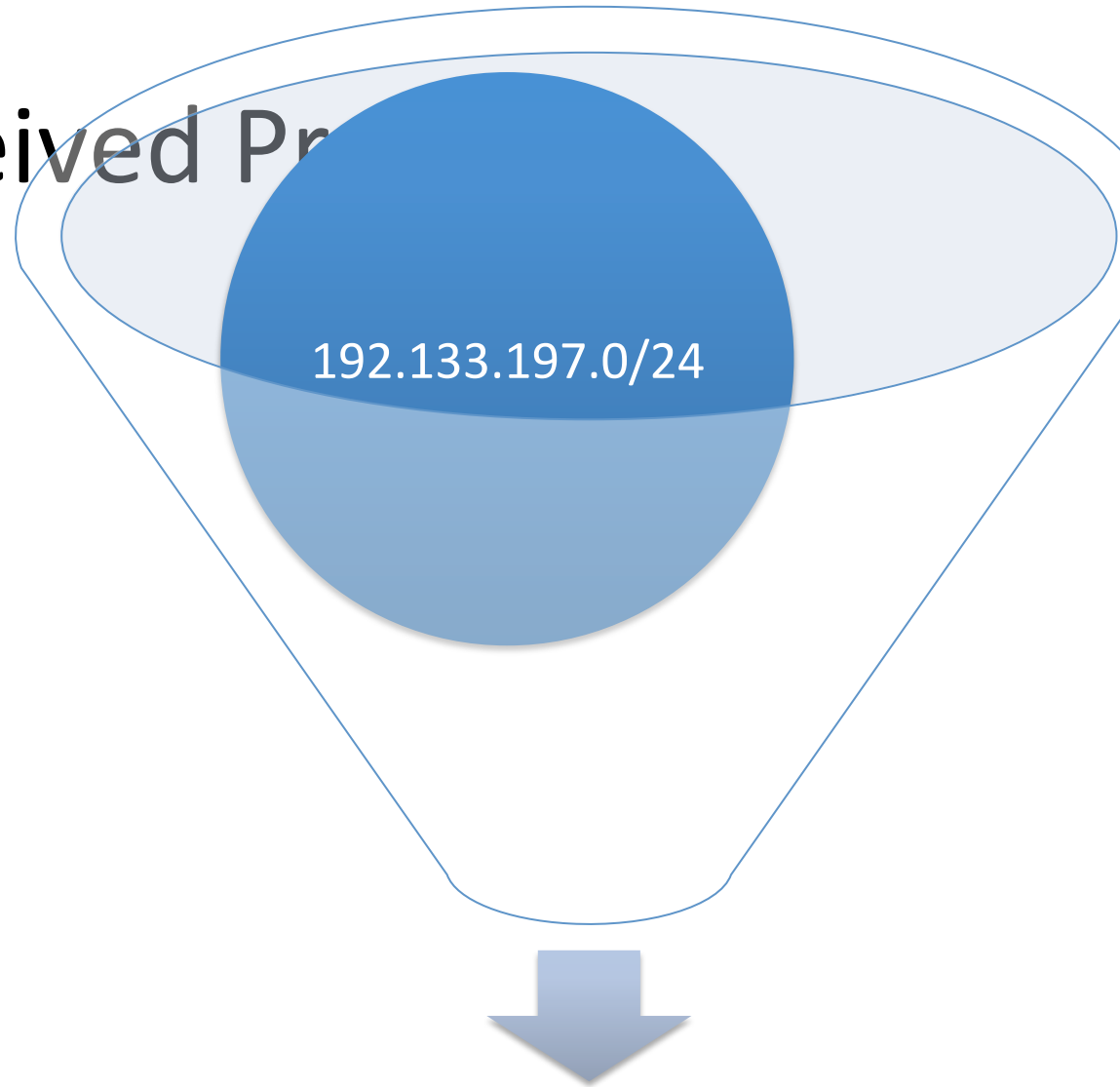
Tim Evens ([tievens@cisco.com](mailto:tievens@cisco.com))

NANOG-65



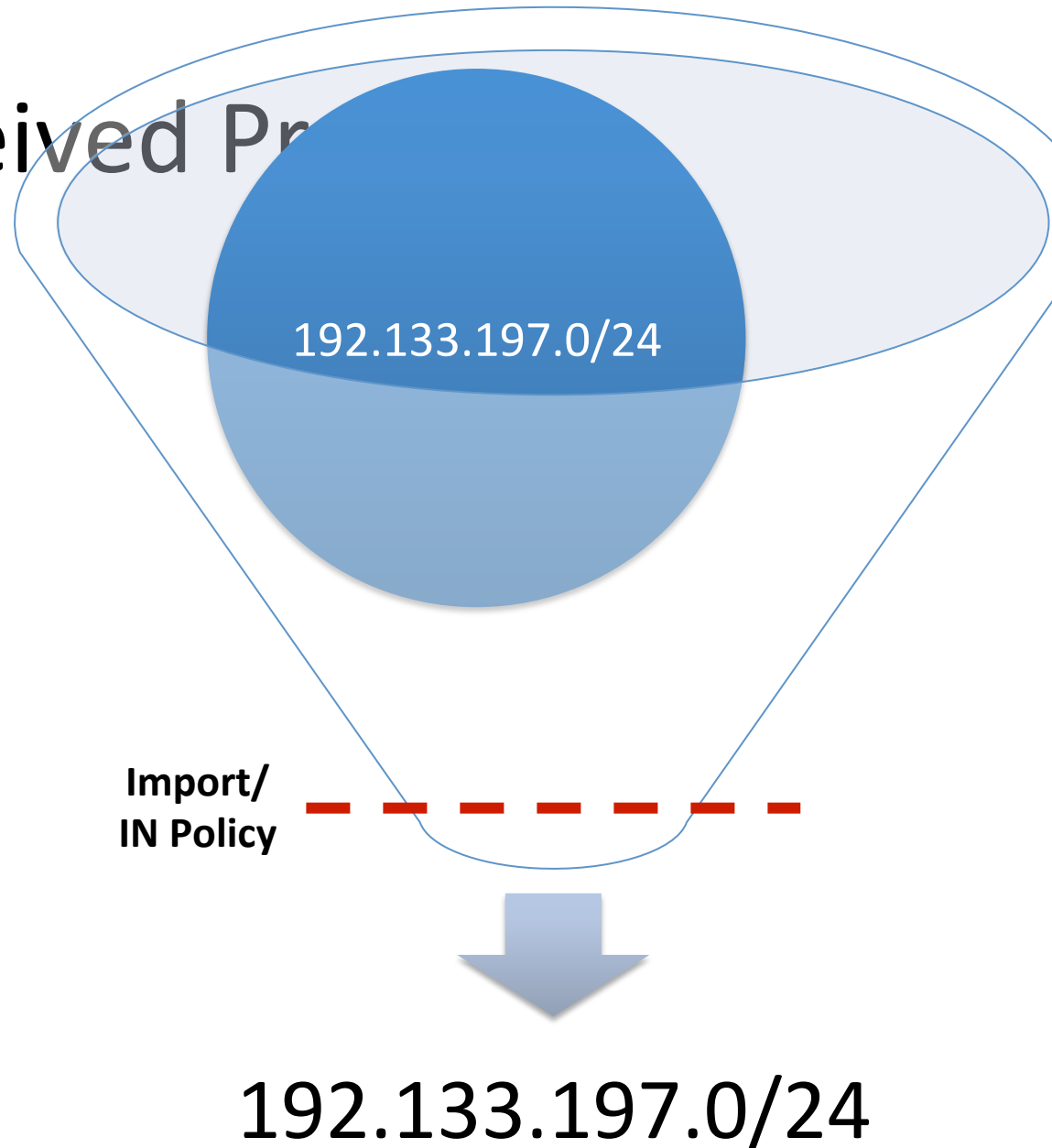
# Received Pr

- Commonly check received prefixes and policy on peer activation



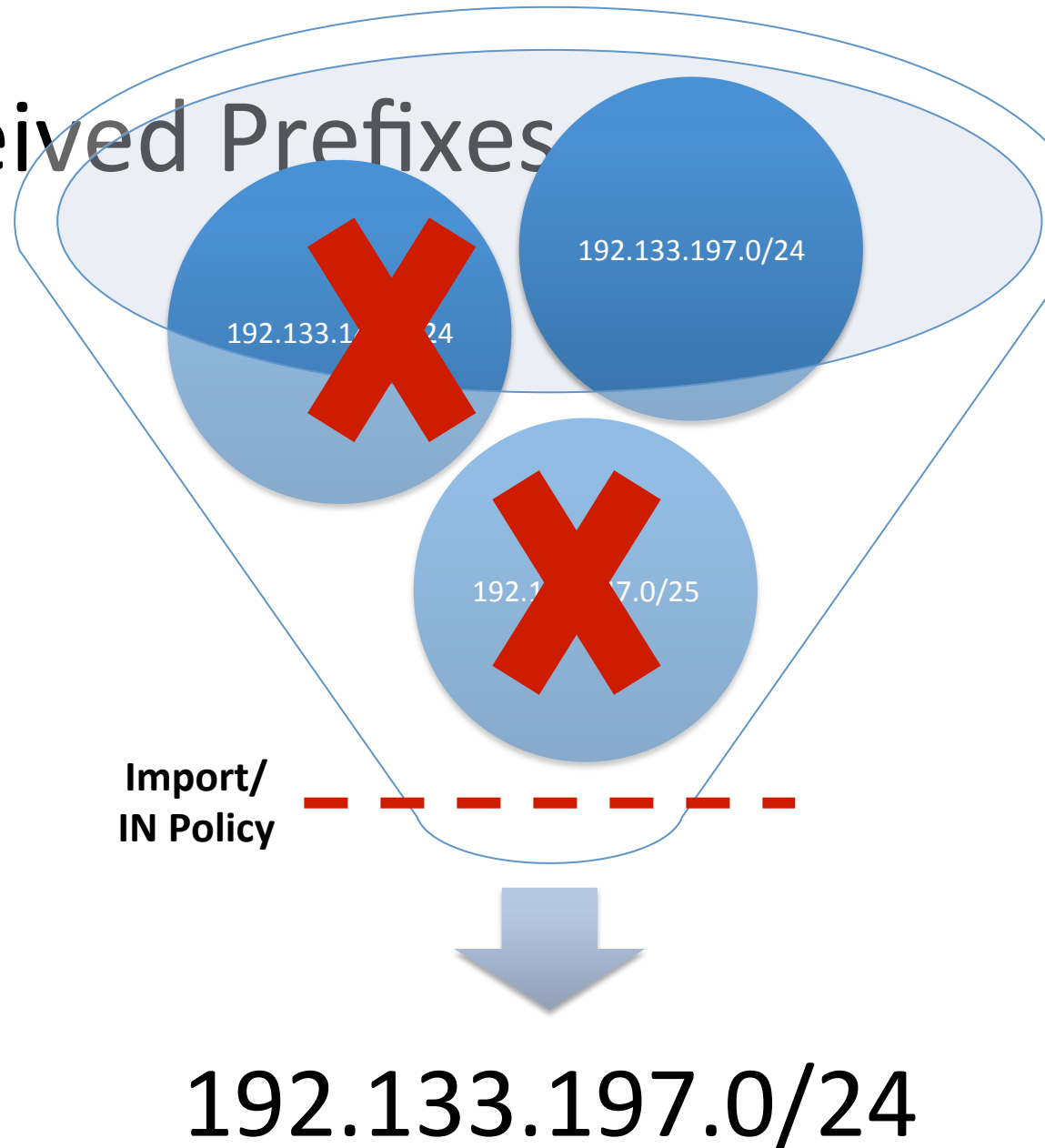
# Received Pr

- Apply policy and permit received prefix



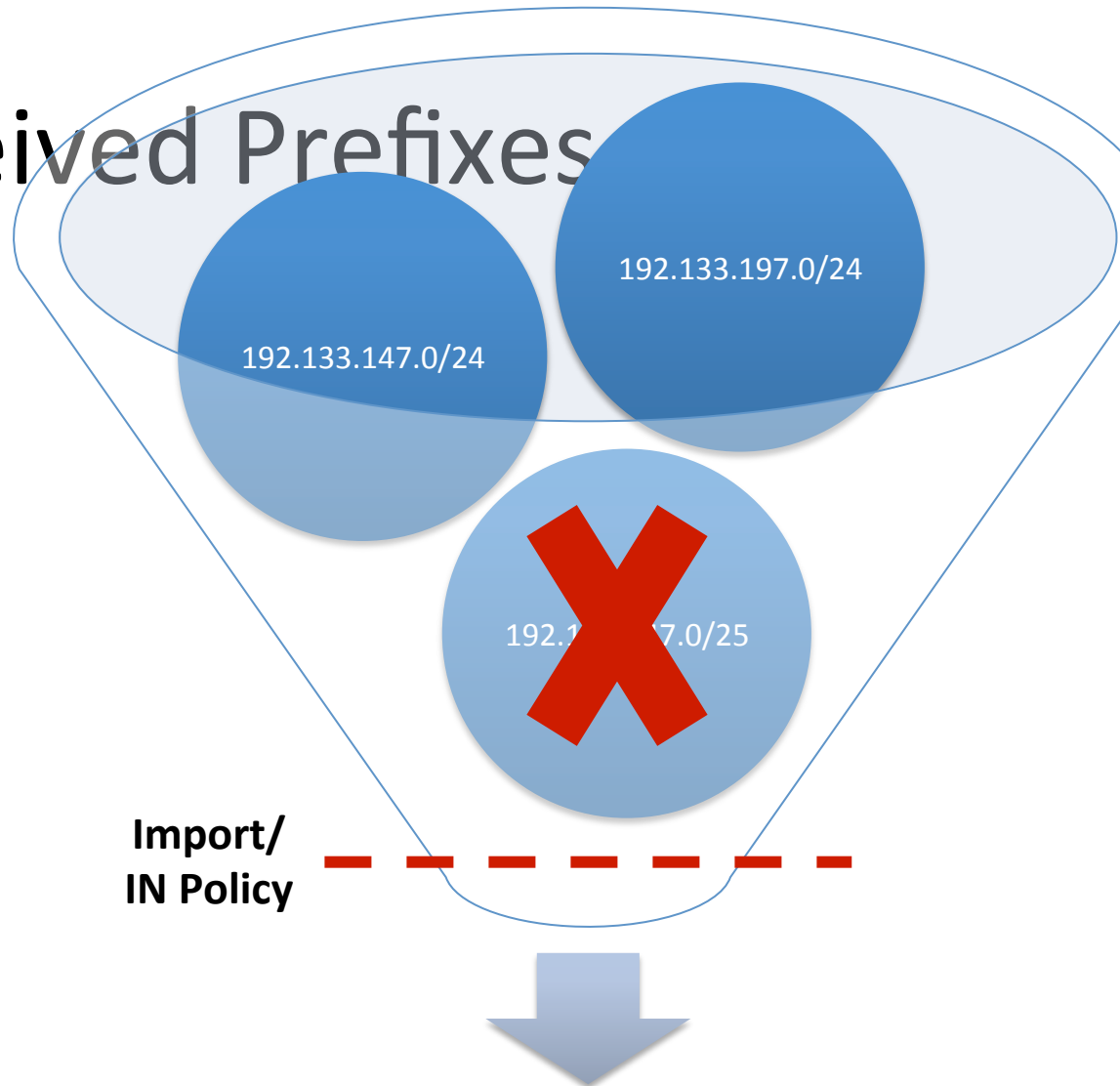
# Received Prefixes

- Days, weeks, months, ... later additional prefixes are received
- Policy is successfully working to prevent additional prefixes
- Does anyone notice



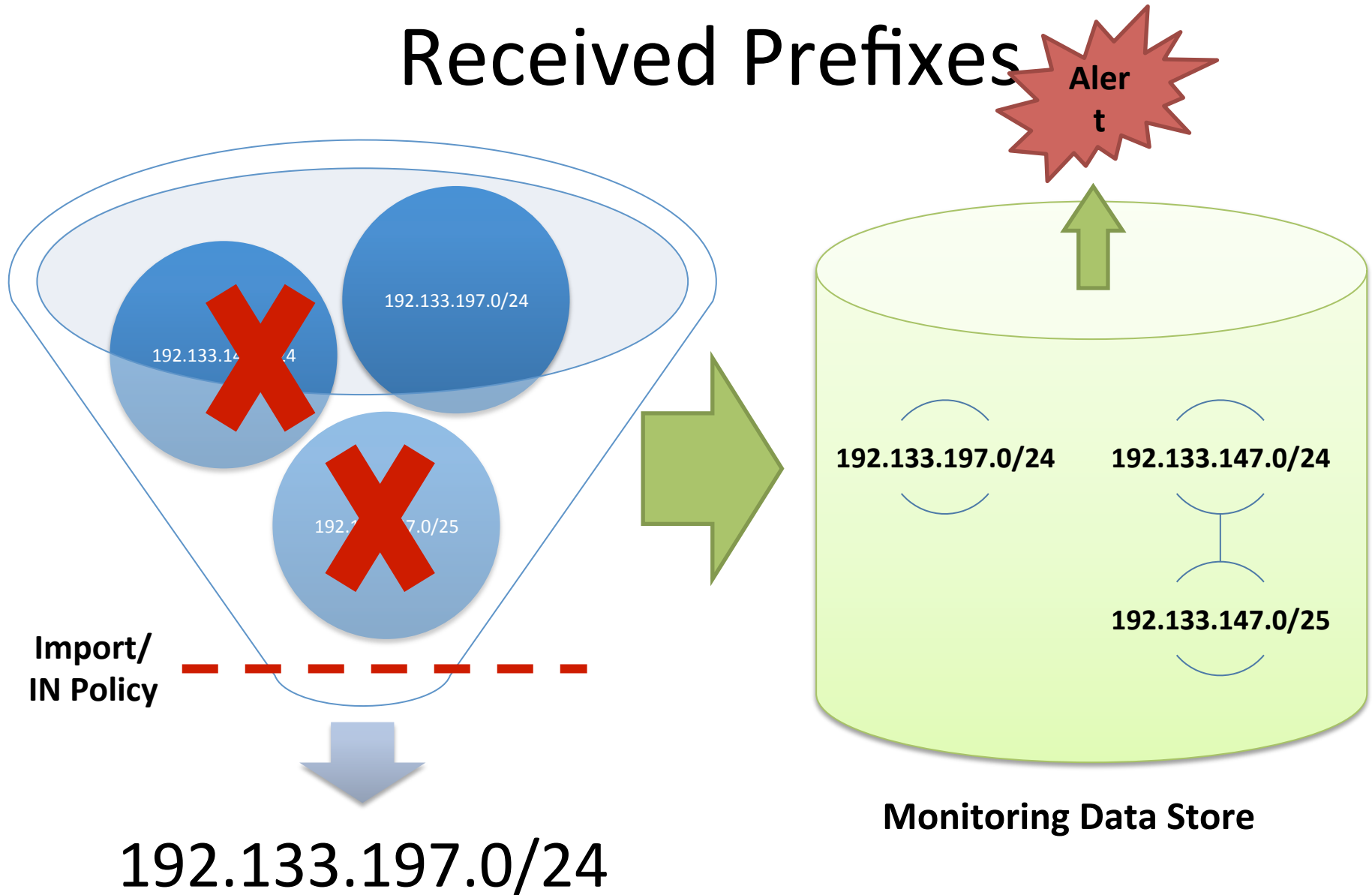
# Received Prefixes

- Prefixes remain received unnoticed
- Policy is changed and no longer filters prefixes that were previously filtered
- 192.133.147.0/24 is leaked

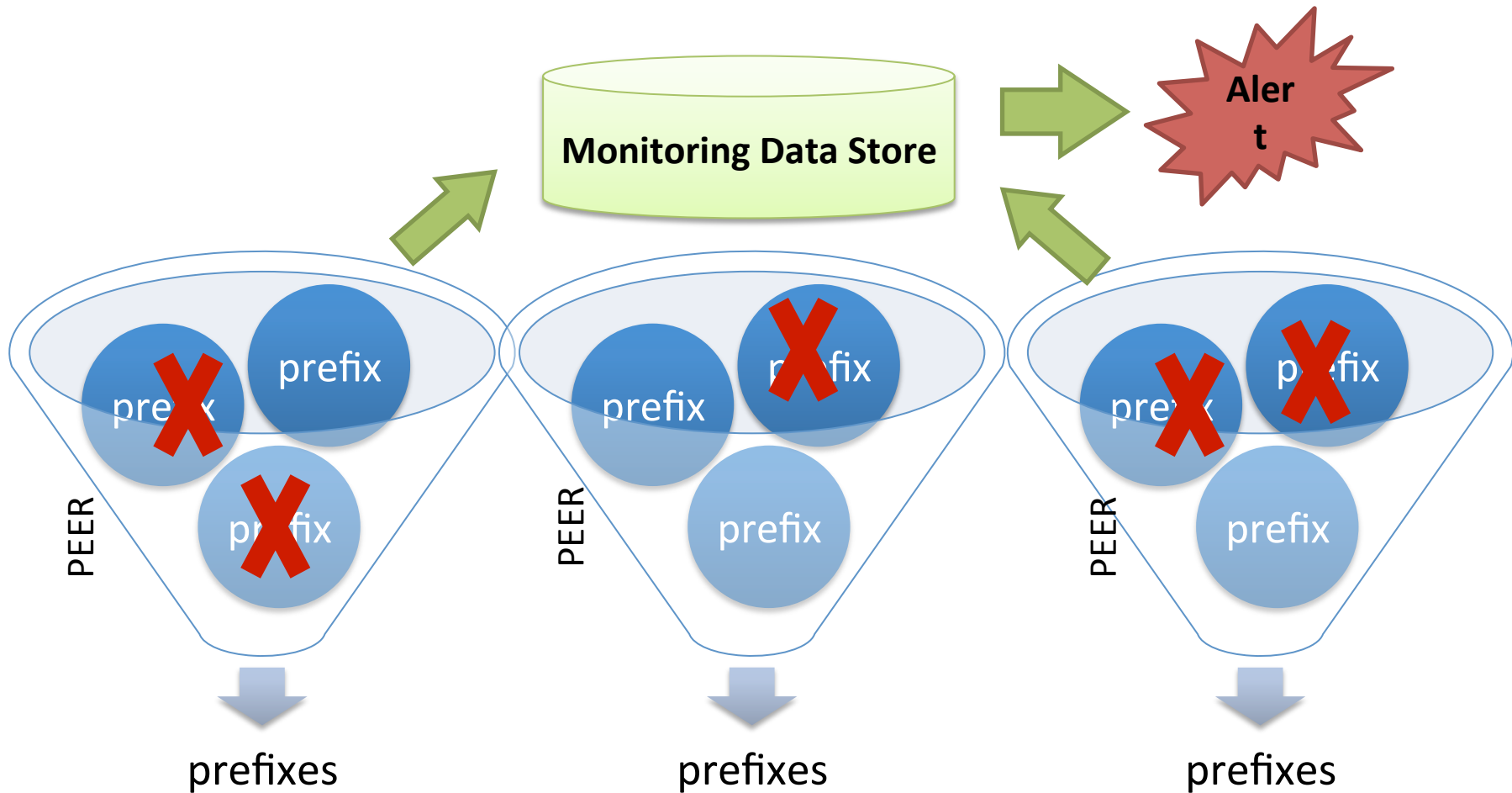


192.133.197.0/24, **192.133.147.0/24**

# Received Prefixes



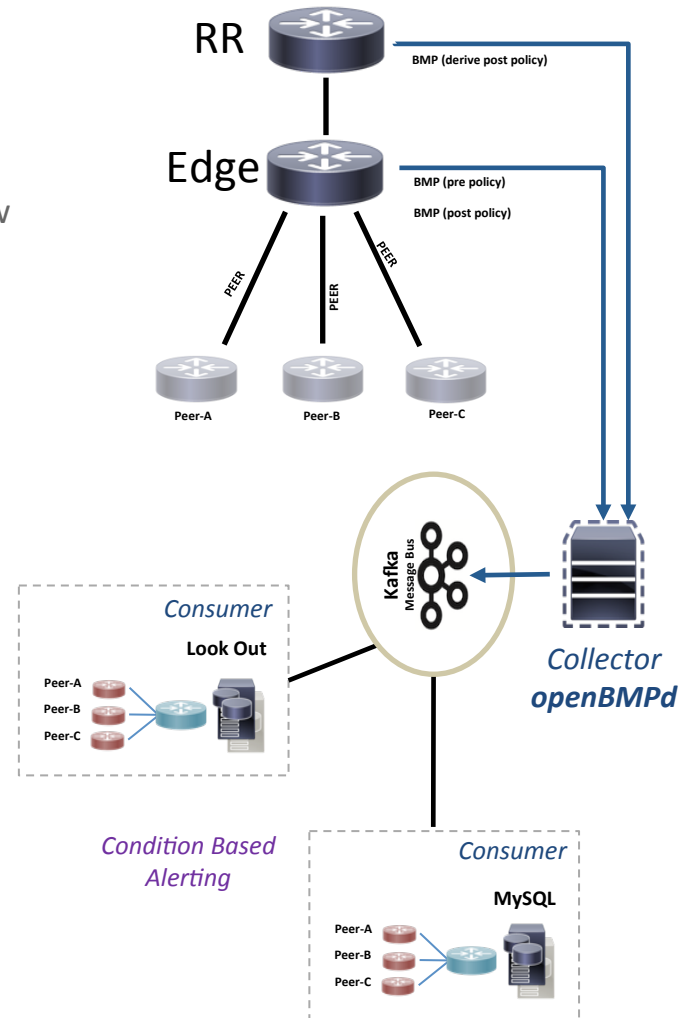
# Peer Type/Role Monitoring



Some prefixes should never be advertised by peer role/type

# Use OpenBMP to Monitor

- OpenBMP is an open-source collector that universally makes available both **parsed** and **RAW** BMP data to any number of applications
- BMP data is forwarded to Apache Kafka in both parsed and BMP raw formats. Any number of consumers can consume this data without requiring multiple BMP feeds from the router
- Baseline/normalize monitoring
- Diff/Compare Edge and RR peering to derive filtered prefixes and alert on filtered prefixes changes
- Apply policy to monitored data in lieu of pre/policy diffs
- Alert when advertisements meet conditions
- [www.openbmp.org](http://www.openbmp.org) and [github.com/openbmp](https://github.com/openbmp)



Questions?





Thank You

**new tacacs!**

morrowc (for andrej/thorsten)

# Updates to the tacacs+ existing draft

Andrej/Thorsten are working to finish the existing draft which expired:

<https://tools.ietf.org/html/draft-grant-tacacs-02>

Their new draft is:

<https://tools.ietf.org/html/draft-dahm-opsawg-tacacs-01>

With security updates and the effort to get this to RFC status.

# Security updates

PSK change capabilities

Transport security

Connection management options

Removal of legacy protocols and legacy methods

Questions to the draft authors:

<https://tools.ietf.org/html/draft-dahm-opsawg-tacacs-01#page-37>

Panel:

How can we work together to improve security and resilience of the global routing system?

# The Panel

- Andree Toonk (BGPmon)
- Job Snijders (NTT)
- Rob Hagens (Zayo)
- Tony Tauber (Comcast)
- Moderator: Andrei Robachevsky (Internet Society)

# Today's discussion

- Inter-domain routing and forwarding
  - Issues and challenges
- Collective responsibility
  - How to address the commons problem?
- Mutually Agreed Norms for Routing Security
  - What it is and can it help?





# Let us briefly look at the problem first

- BGP is based on trust
  - No validation of the legitimacy of updates
  - Chain of trust spans continents
  - Lack of reliable resource data
  - BGPSEC is under development in the IETF



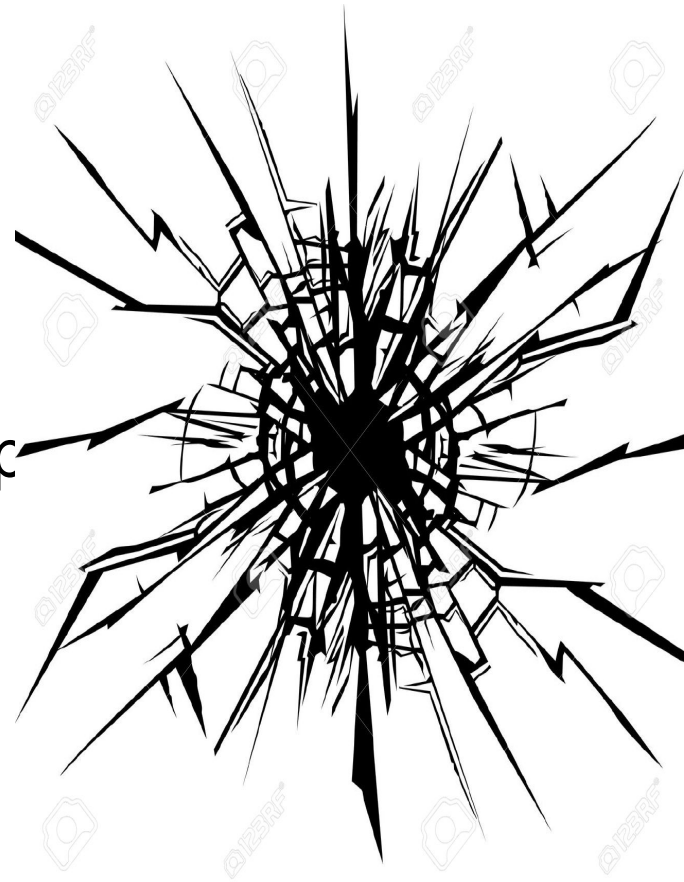
## But also

- Source IP address spoofing
  - Forging the source IP address of packets
- Collaboration
  - How do you reach someone on the other side of the Net to help you out?
  - How do you mitigate a DDoS?



# Impact

- Prefix hijack
  - Denial of service, impersonating a network or a service, traffic interception
- “Route leak”
  - Traffic intercept, but may result in denial of service
- IP spoofing
  - The root cause of reflection DDoS attacks



How severe is the problem of lack of routing security in today's inter-domain routing?

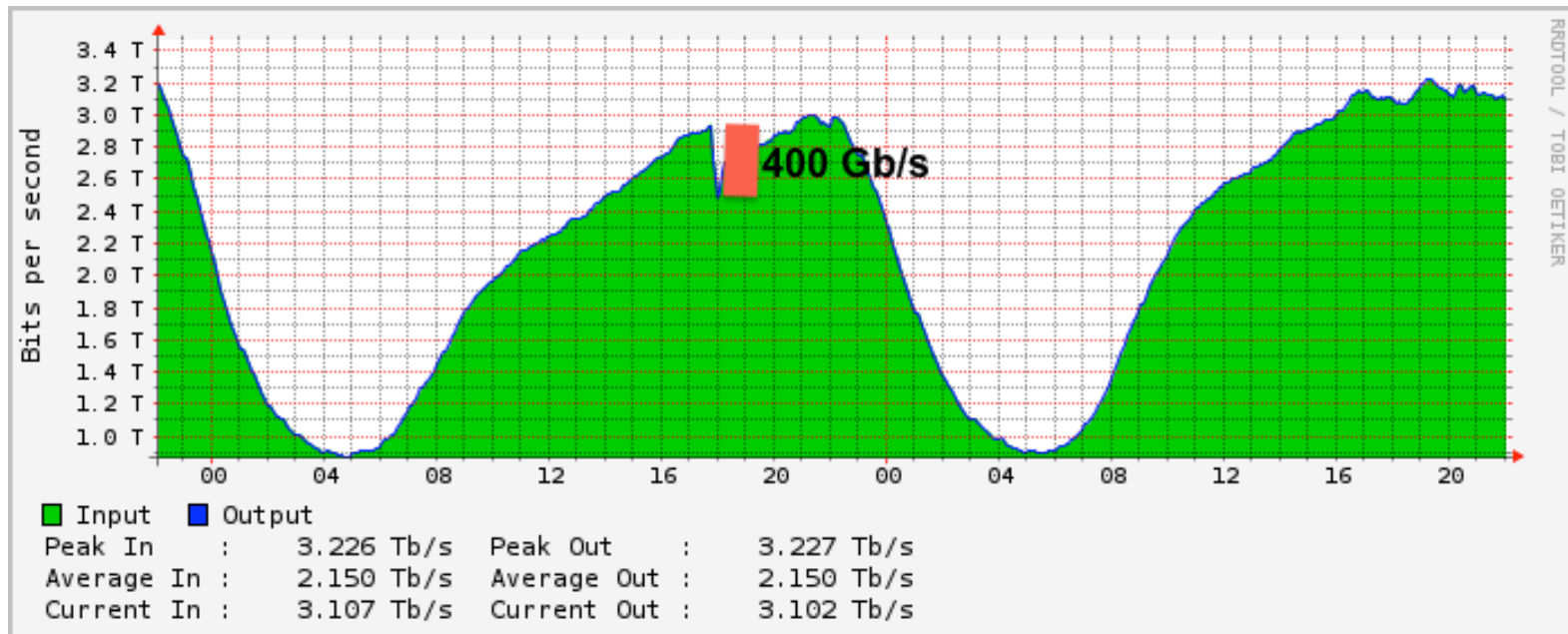
# BGP hijack

- *“Someone other than your AS, or other than someone you gave authorization , is announcing your prefix”*
- Youtube hijack
- Spammers
- Governments for censorship
- etc



# Losing 400Gb/s

Announcing Peering Lan prefixes, big problem for Internet Exchange points



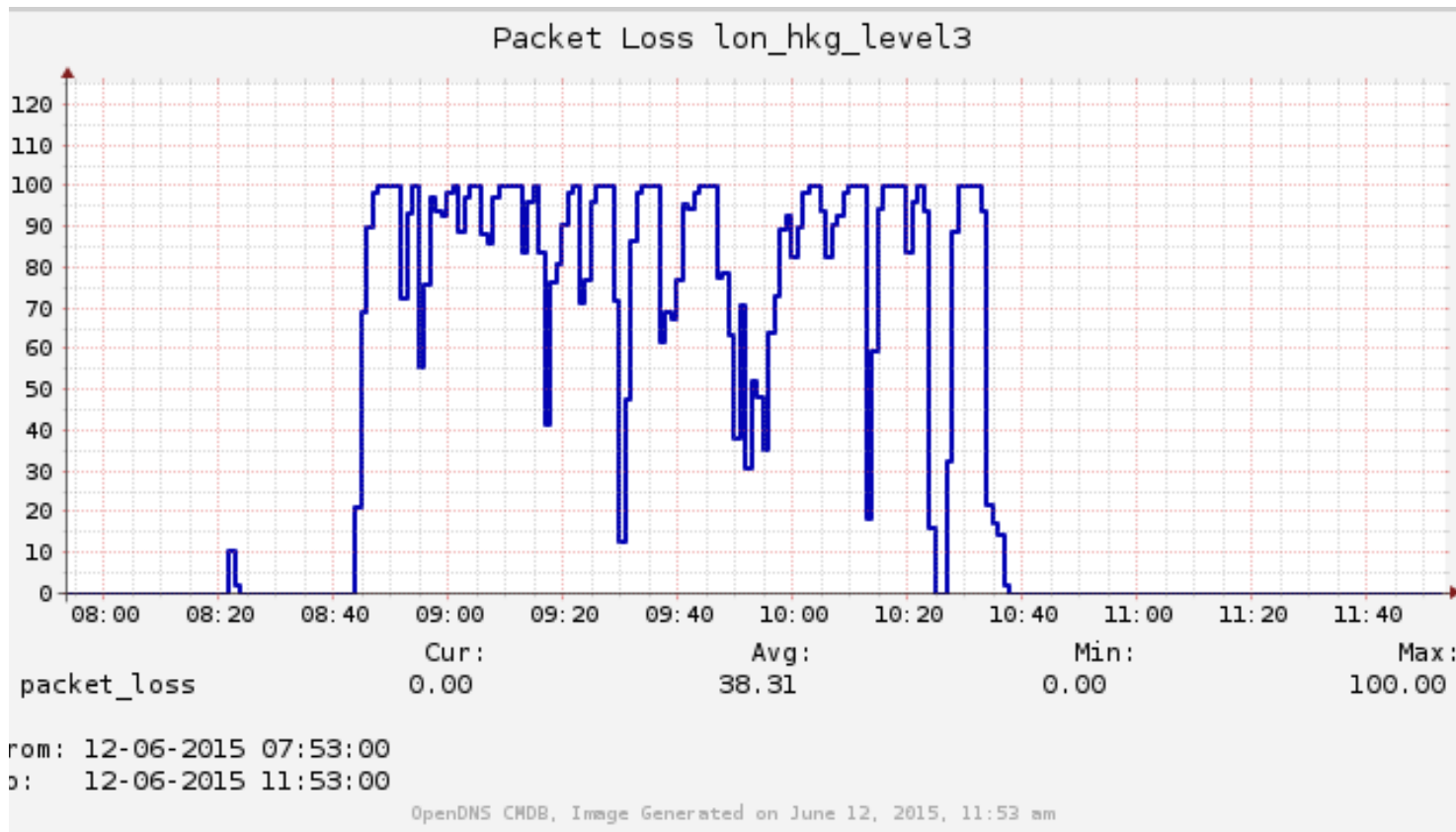
# BGP leaks





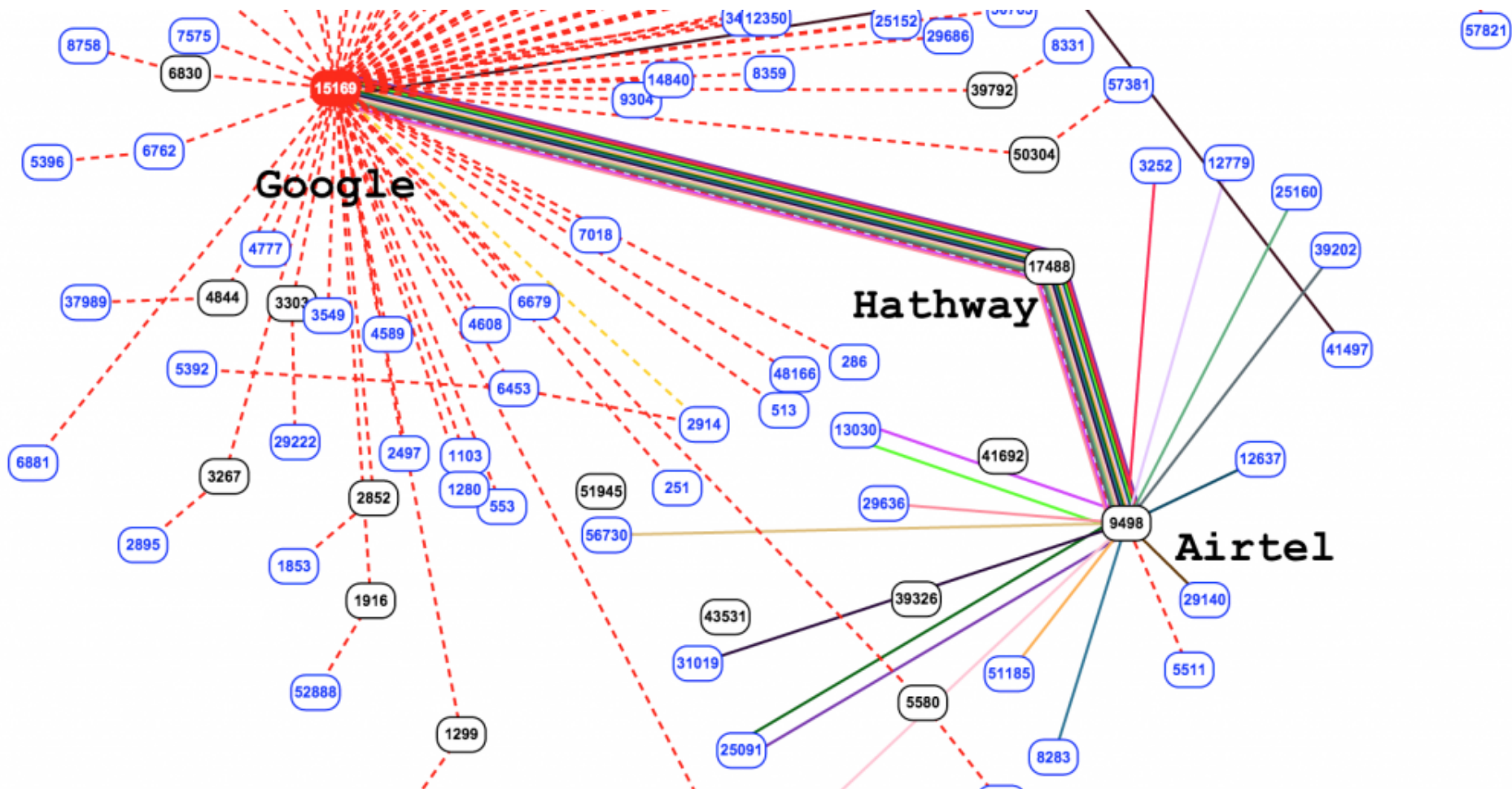
# Telekom Malaysia bgp leak

June 12. Telekom Malaysia (AS4788) Leaked 179,000 of prefixes to Level3 (AS3549)  
Resulted in significant packet loss, instability and Internet slow down in all parts of the world.





# Google prefixes leaked and routed via India



# What is available to address these problems?

- Tools

- Prefix and AS-PATH filtering, RPKI, IRR, ...
- Ingress and egress anti-spoofing filtering, uRPF, ...
- Coordination and DDoS mitigation

- Challenges

- Your safety is in someone else's hands.

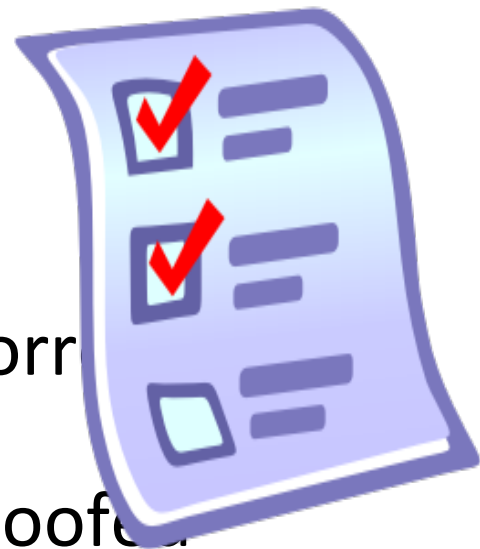
Implementing control plane fixes at just one network to network interface does not resolve the problem.

# Mutually Agreed Norms for Routing Security (MANRS)

- MANRS builds a visible community of security-minded operators
  - Promotes culture of collaborative responsibility
- Defines four concrete actions that network operators should implement
  - Technology-neutral baseline for global adoption



# Good MANRS



1. Filtering – Prevent propagation of incorrect routing information.
2. Anti-spoofing – Prevent traffic with spoofed source IP addresses.
3. Coordination – Facilitate global operational communication and coordination between network operators.
4. Global Validation – Facilitate validation of routing information on a global scale.

# 1. Filtering

## Prevent propagation of incorrect routing information

*Network operator defines a clear routing policy and implements a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with prefix and AS-path granularity.*

*Network operator is able to communicate to their adjacent networks which announcements are correct.*

*Network operator applies due diligence when checking the correctness of their customer's announcements, specifically that the customer legitimately holds the ASN and the address space it announces.*

## 2. Anti-Spoofing

### Prevent traffic with spoofed source IP address

*Network operator implements a system that enables source address validation for at least single-homed stub customer networks, their own end-users and infrastructure. Network operator implements anti-spoofing filtering to prevent packets with an incorrect source IP address from entering and leaving the network.*

# 3. Coordination

Facilitate global operational communication and coordination between the network operators

*Network operators should maintain globally accessible up-to-date contact information.*

## 4. Global Validation

- Facilitate validation of routing information on a global scale.

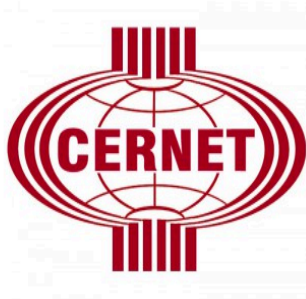
*Network operator has publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties.*












































# MANRS is not (only) a document – it is a commitment

- 1) The company supports the Principles and implements at least one of the Actions for the majority of its infrastructure.
- 2) The company becomes a Participant of MANRS, helping to maintain and improve the document and to promote MANRS objectives

# Public launch of the initiative - 6 November 2014



# A growing list of participants

	Country	ASNs	Filtering	Anti-spoofing	Coordination	Global Validation
KPN	NL	1136, 5615, 8737				
Seeweb	IT	12637				
Gigas	ES, US	57286, 27640				
NTT	US	2914				
BIT BV	NL	12859				
Algar Telecom	BR	16735, 53006, 27664				
OpenCarrier eG	DE	41692				
SpaceNet	DE	5539				
CERNET	CN	4538				
SpeedPartner GmbH	DE	34225				
Comcast	US	7015, 7016, 7725, 7922, 11025, 13367.				

# Are you interested in participating?

**Filtering**



**Anti-Spoofing**



**Coordination**



**Global scale**



# I suspect some of you are asking yourself

- My company has always taken security seriously, we've implemented many of the Actions and much more long time ago...
- - Why joining MANRS now? What difference will it make?

# Is any of these a good reason?

Because routing security is a sum of all contributions

Because this is a way to demonstrate a new baseline

Because a community has gravity that can attract others

What are the challenges?  
implementation, compliance  
checks, credibility

What useful activities  
can be built around MANRS?



# What the participants say

- *Adherence to MANRS is an important commitment that operators make back to the Internet community. Together we aim to remove the havens from which miscreants maintain the freedom and anonymity to attack our network and our customers. David Freedman, Claranet Group*
- *Comcast is committed to helping drive improvements to the reliability of the Internet ecosystem. We are thrilled to be engaged with other infrastructure participants across the spectrum and around the globe in pursuit of these goals. Jason Livingood, Vice President, Internet Services, Comcast*
- *Zayo is interested and desires to be more active in promoting global routing security; the MANRS document is in our (and my) opinion a really good initial level of recommendations. I think that the more participation in MANRS, the safer our routing ecosystem. And a safer routing system is good for all of us! Robert Hagens, VP, IP Architecture, Zayo*
- *Cogent supports the efforts championed by the MANRS document. The issues being promoted need practical, effective improvements to support the continued growth and reliance on the Internet. Hank Kilmer, Cogent*
- *As one of the most connected Internet providers in the world, security of the Internet is top-of-mind at Level 3 Communications. The Internet is a shared responsibility, and only through these important collaborative efforts can we continue to ensure the protection of this collective infrastructure. Dale Drew, Senior Vice President, Chief Security Officer at Level 3 Communications.*
- *We believe that the objectives and scope match our beliefs and our behaviour, and that by signing up, we may help encourage others to do so. Ian Dickinson, Network Architect, Sky*
- *Good network routing practice is the fundamental requirement for trust between providers, and ultimately creates a safer and stronger internet for customers. KPN is committed to providing secure and trustworthy communications, and by joining partners in MANRS, we continue to improve security and resiliency for all. – Jaya Baloo, Chief Information Security Officer, KPN*
- *We believe in the value of coordination and shared responsibility to have a more secure Internet infrastructure. We strongly agree with the principles, the scope and the actions written in the*



MANRS

# Routing Resilience Manifesto, aka MANRS

<https://www.routingmanifesto.org/>

<https://www.manrs.org/>

Thank you!

NANOG 65 – Security Track