MANRS

MANRS

Mutually Agreed Norms for Routing Security

Aftab Siddiqui

siddiqui@isoc.org

The Problem

A Routing Security Overview

Routing Incidents are Increasing

In 2017 alone, 14,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more.

About 40% of all network incidents are attacks, with the mean duration per incident lasting 19 hours.

Incidents are global in scale, with one operator's routing problems cascading to impact others.

Routing Incidents Cause Real World Problems

Insecure routing is one of the most common paths for malicious threats.

Attacks can take anywhere from hours to months to even recognize.

Inadvertent errors can take entire countries offline, while attackers can steal an individual’s data or hold an organization’s network hostage.

The Basics: How Routing Works

There are ~60,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

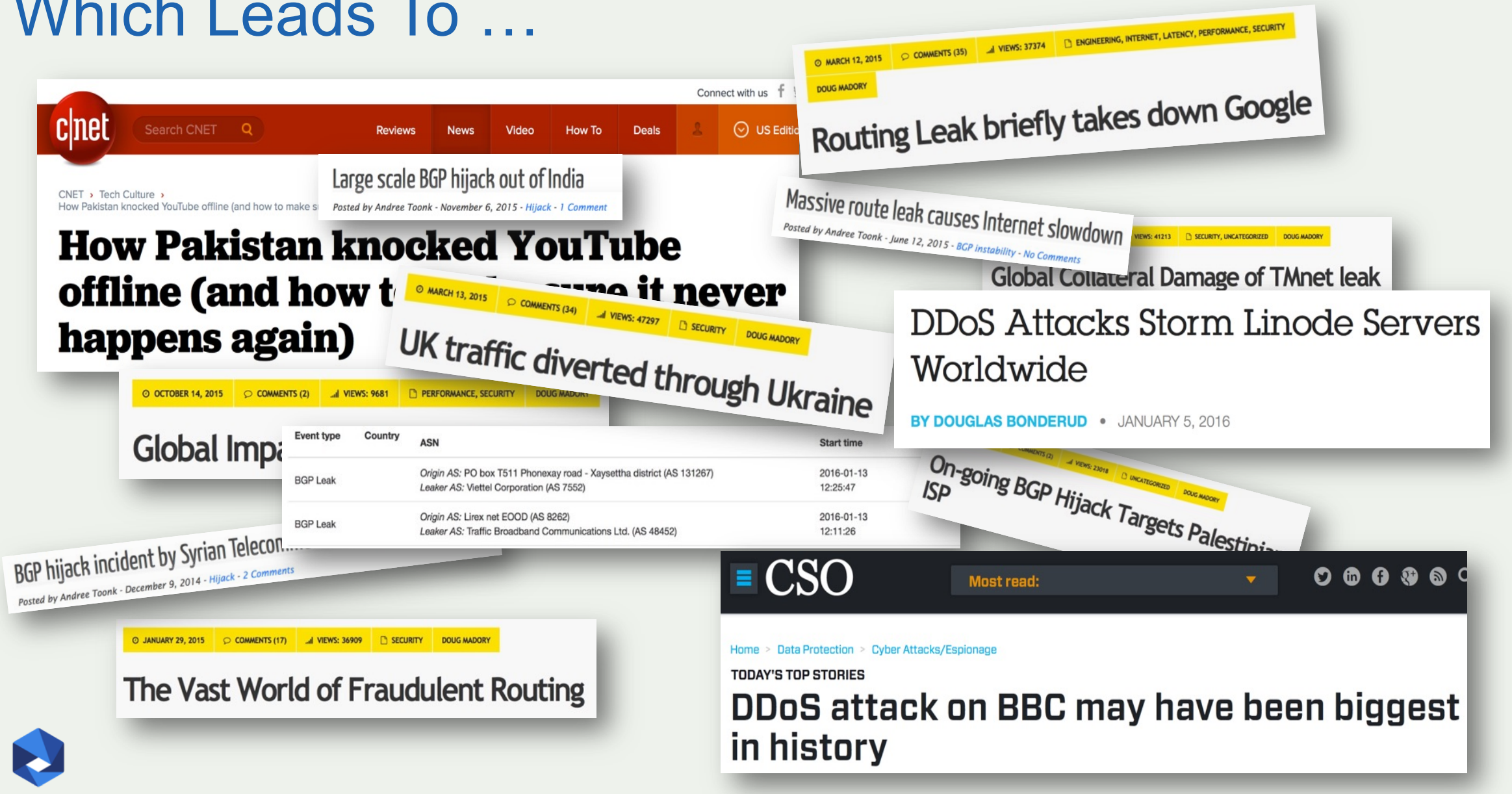
Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

The Honor System: Routing Issues

Border Gateway Protocol (BGP) is based entirely on trust between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

Which Leads To …



EDITION: AS

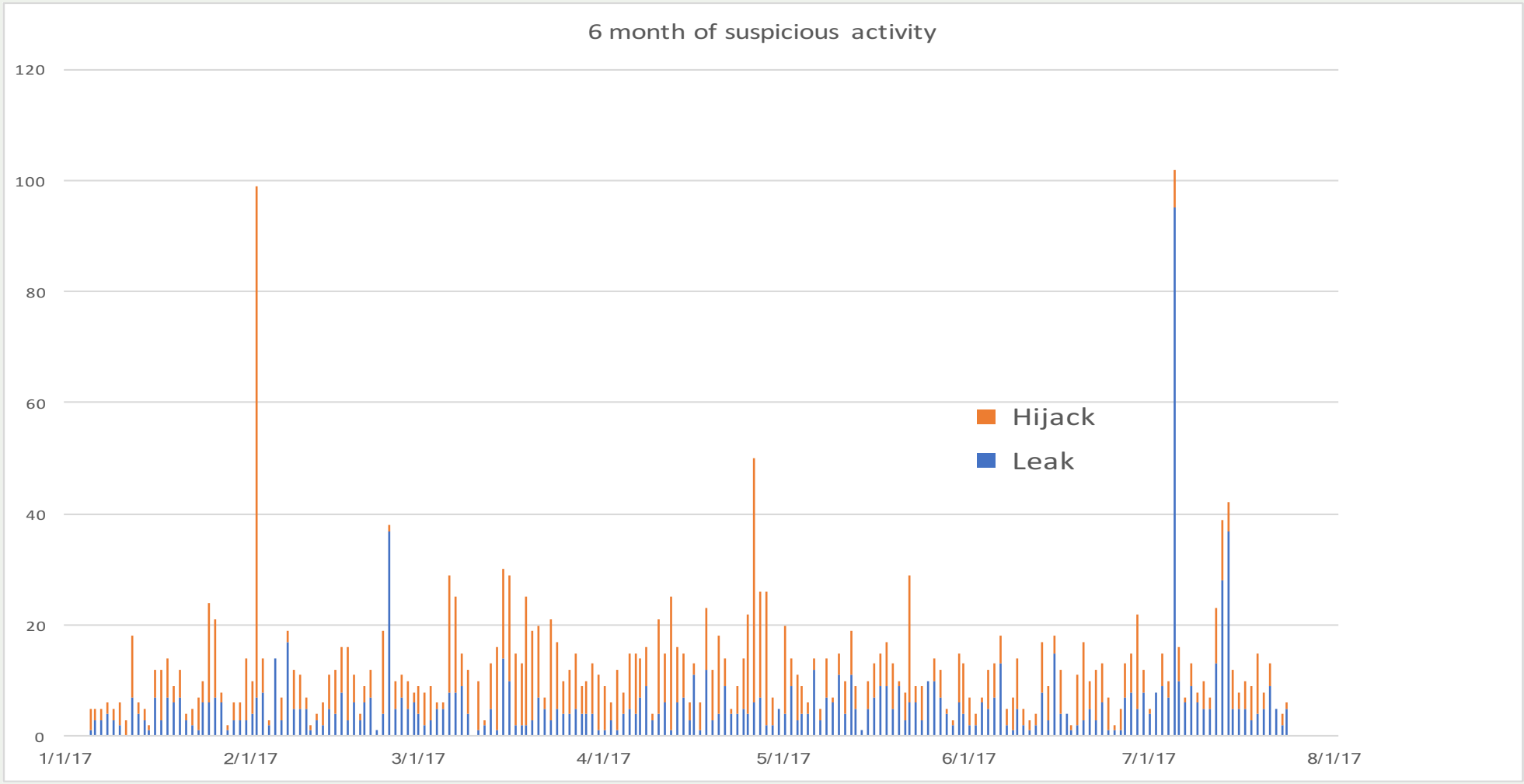
ZDNet

SECURITY CLOUD STORAGE CXO HARDWARE MICROSOFT INNOVATION MORE NEWSLETTERS

MUST READ I ASKED APPLE FOR ALL MY DATA. HERE'S WHAT WAS SENT BACK

AWS traffic hijack: Users sent to phishing site in two-hour cryptocurrency heist

No Day Without an Incident



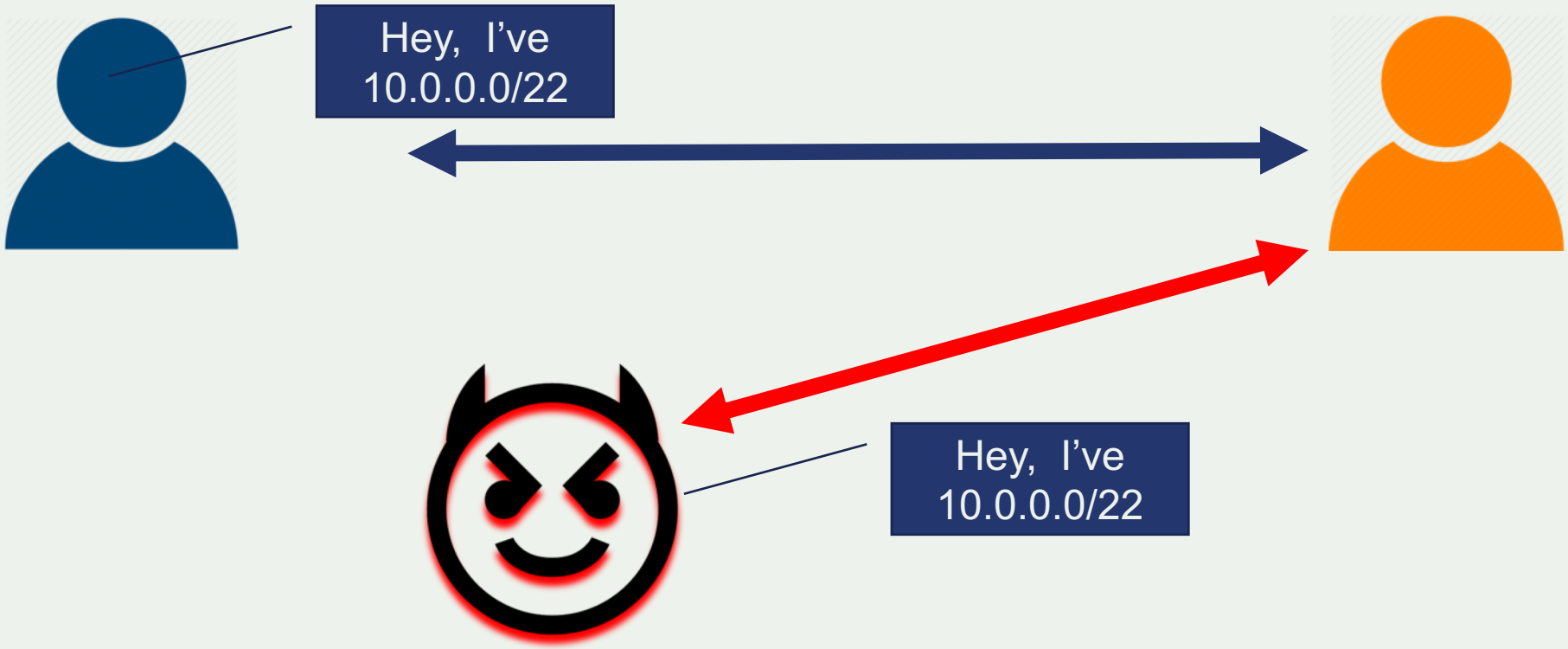
http://bgpstream.com/

The Threats: What's Happening?

Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	Source address validation

Route/Prefix Hijacking

Somebody else sending BGP messages that contain (part of) your IP address ranges

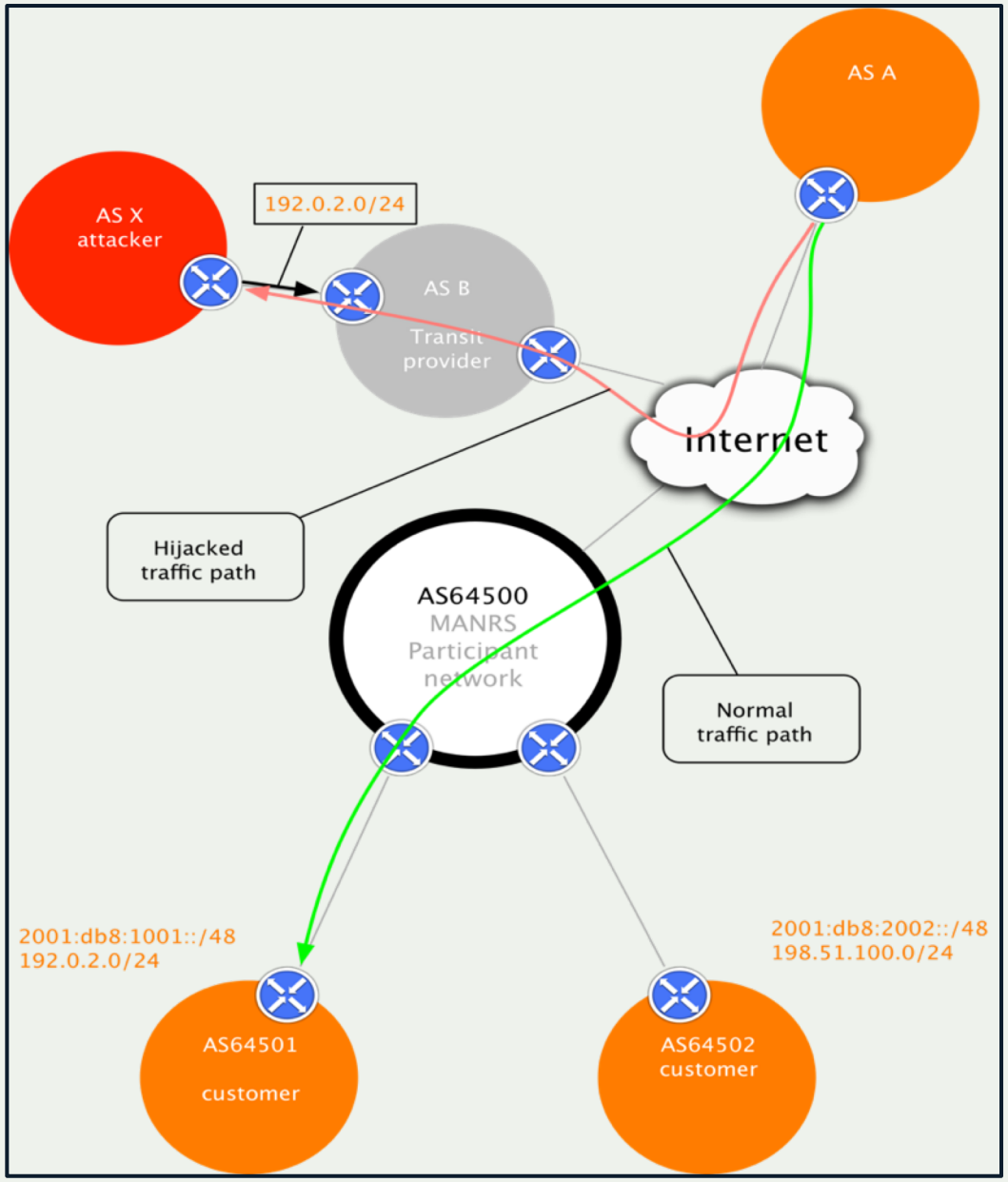


Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or network is their client. This routes traffic to a network operator, when another real route is available.

Example: The 2008 YouTube hijack; an attempt to block YouTube through route hijacking led to much of the traffic to YouTube being dropped around the world.

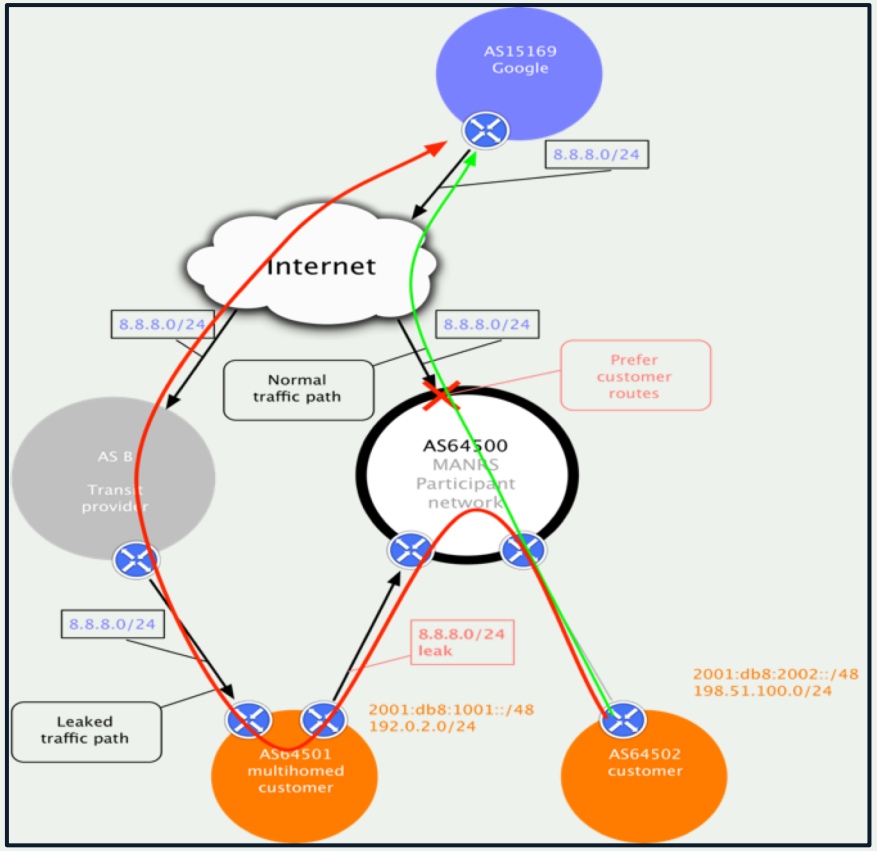
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting false announcements).



Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.



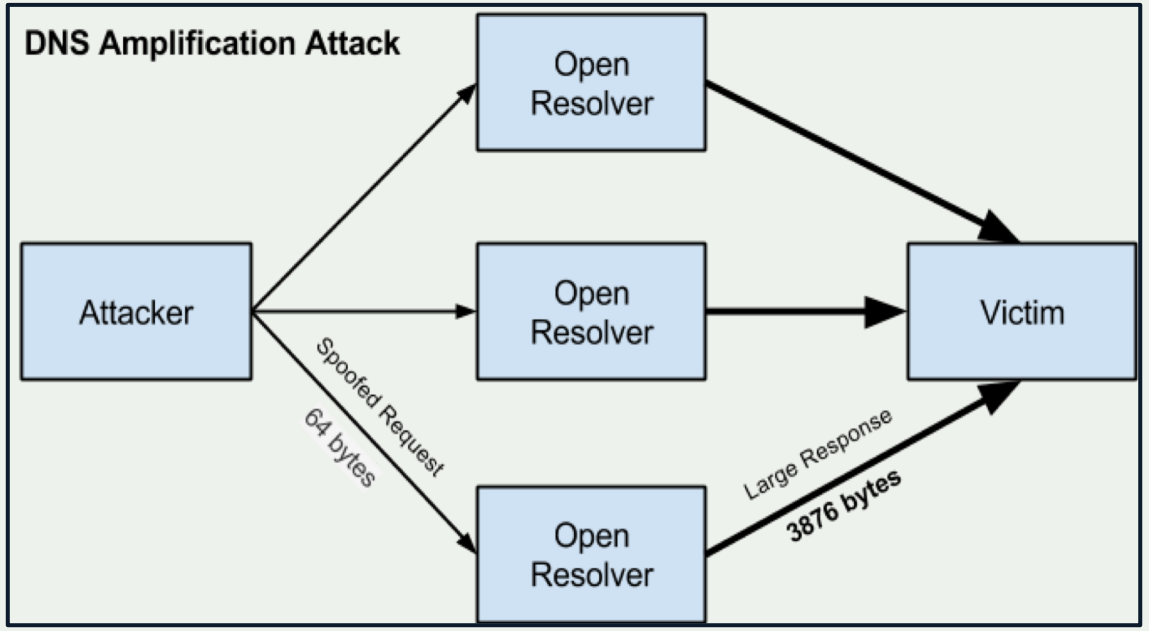
Fix: Strong filtering policies (adjacent networks should strengthen their filtering policies to avoid accepting announcements that don't make sense).

IP Address Spoofing

IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.

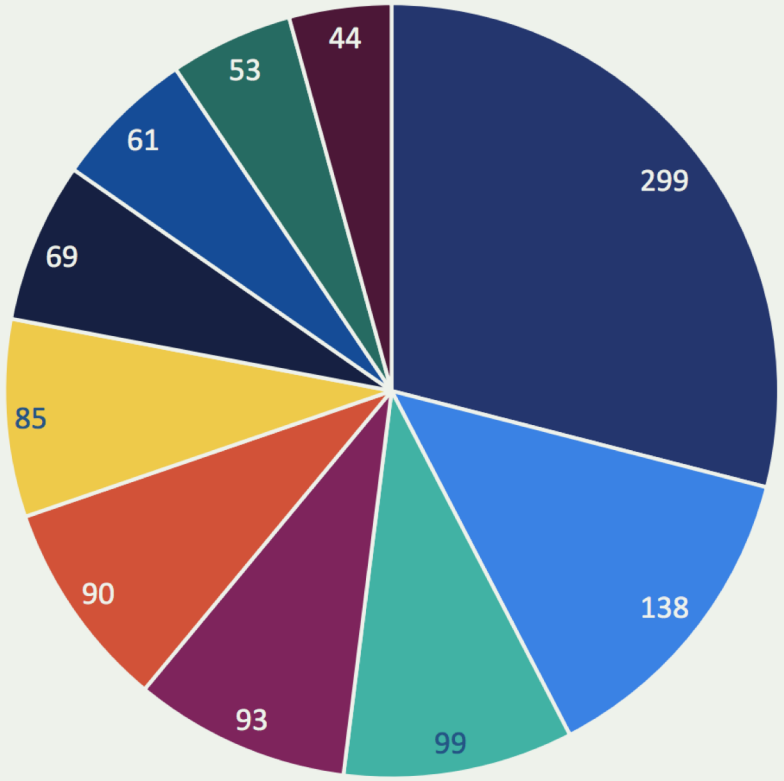
Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).



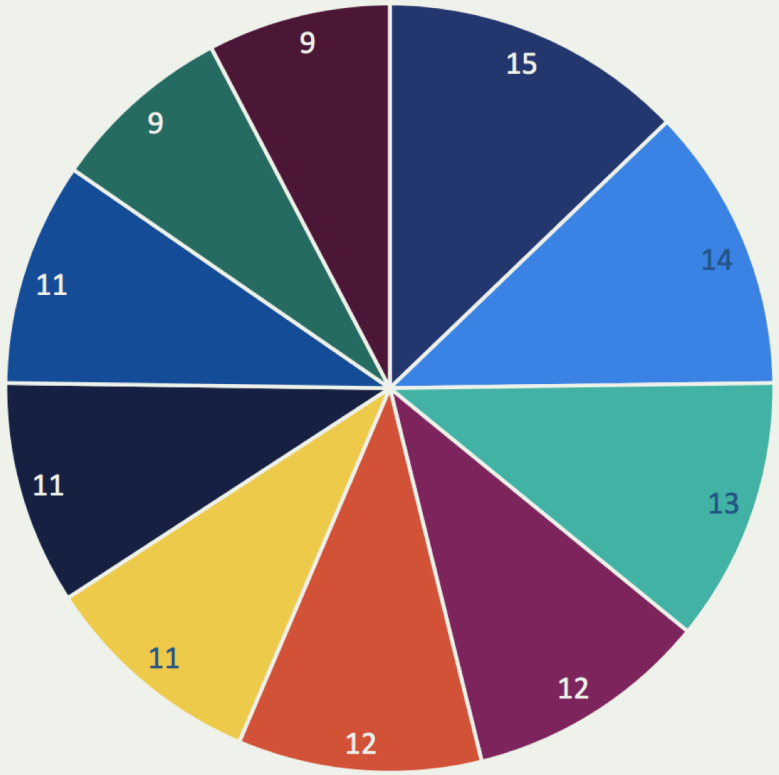
Routing Incidents: 2017

APAC: potential victims

Incidents with a victim in a country, Top 10



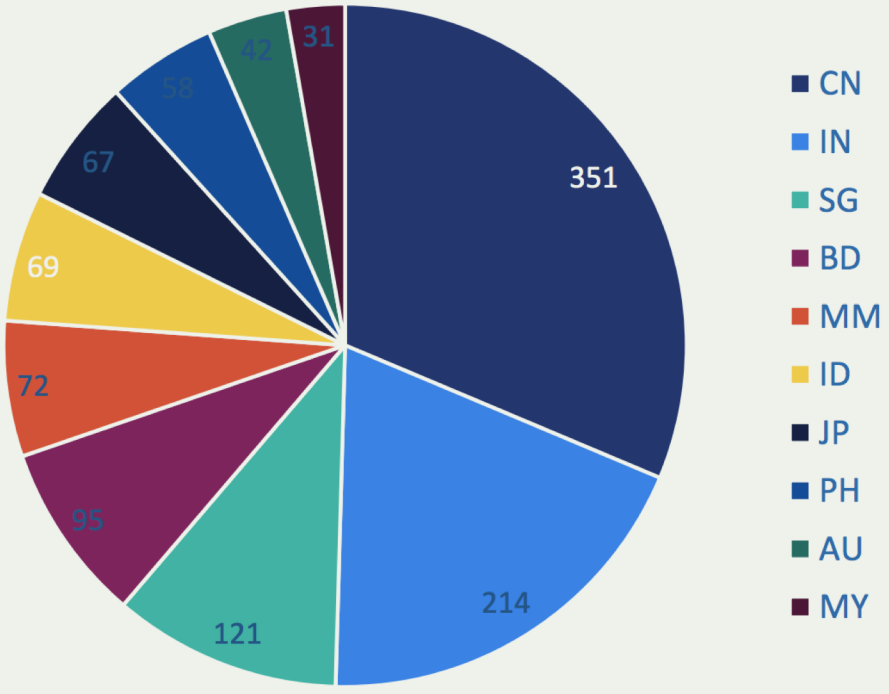
Top 10 victims of routing incidents



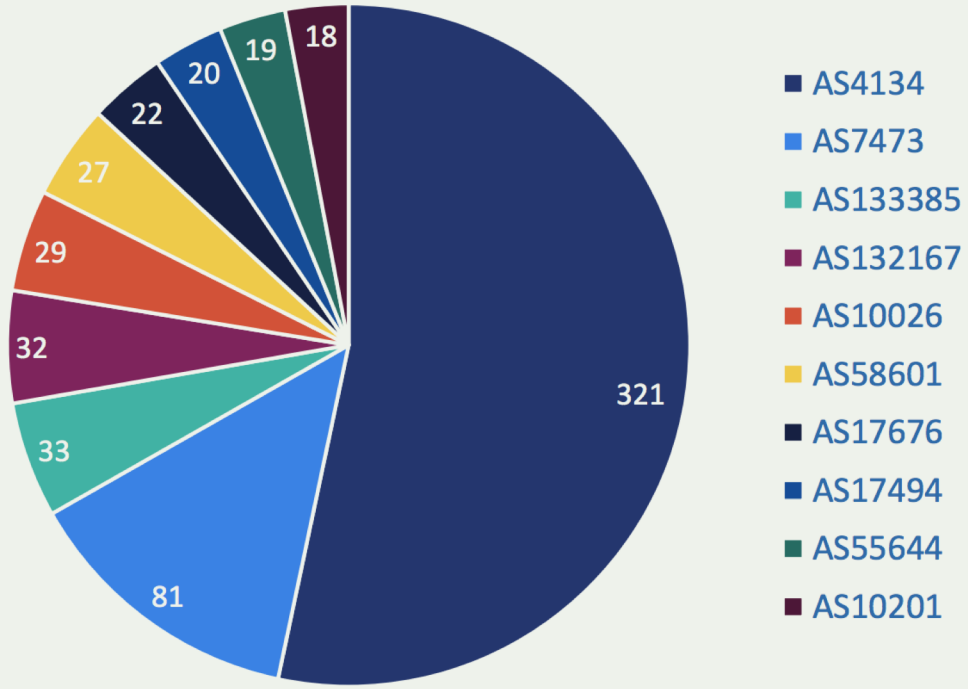
Routing Incidents: 2017

APAC: potential culprits

Incidents with a culprit in a country, top 10

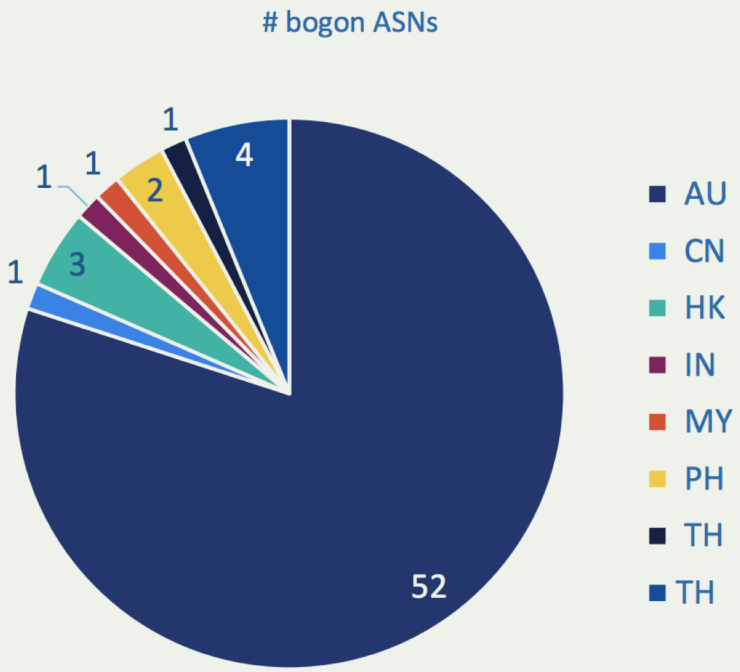


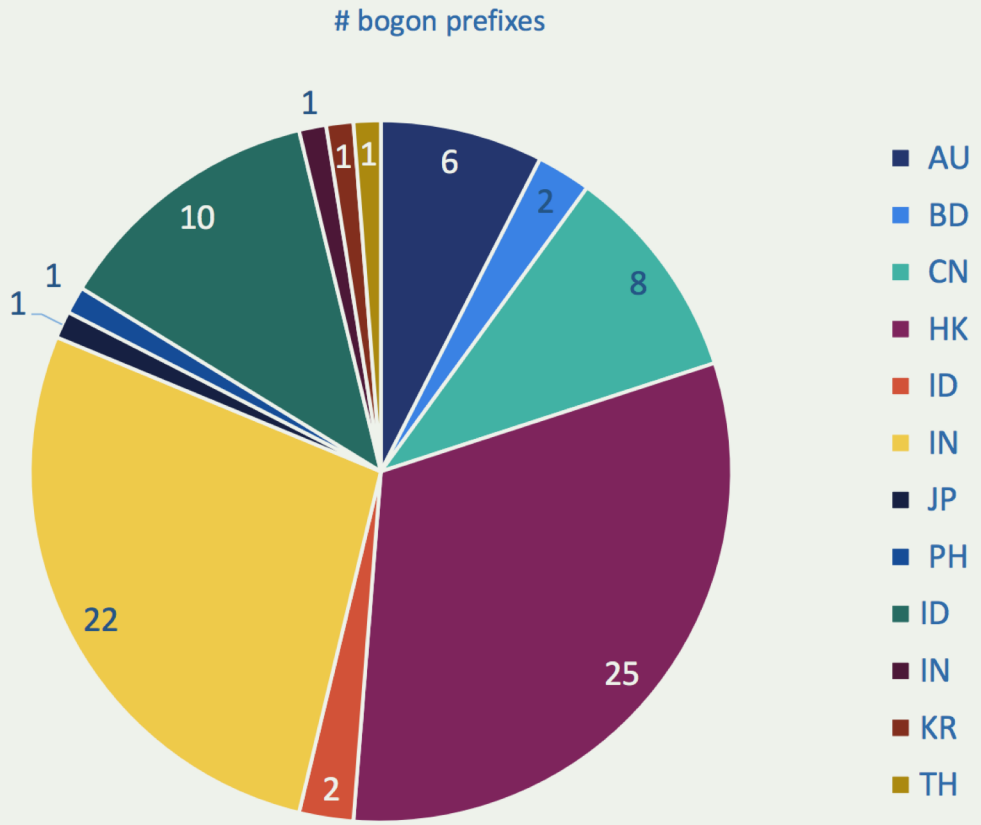
Top 10 potential culprits in routing incidents



Routing Incidents

Bogons: APAC





Bogons

Source: www.cidr-report.org

45.124.164.0/22	AS38803	GTELECOM-AUSTRALIA	Gtelecom-AUSTRALIA,	AU	45.124.164.0	45.124.167.255
45.252.236.0/22	AS38803	GTELECOM-AUSTRALIA	Gtelecom-AUSTRALIA,	AU	45.252.236.0	45.252.239.255
103.20.219.0/24	AS55795	VERBDC1-AS-AP	Verb	AU	103.20.219.0	103.20.219.255
103.24.196.0/22	AS24130	TPG-AU	TPG	AU	103.24.196.0	103.24.199.255
103.58.216.0/22	AS38803	GTELECOM-AUSTRALIA	Gtelecom-AUSTRALIA,	AU	103.58.216.0	103.58.219.255
103.221.236.0/22	AS38803	GTELECOM-AUSTRALIA	Gtelecom-AUSTRALIA,	AU	103.221.236.0	103.221.239.255
220.152.112.0/21	AS23871	AINS-AS-AP	Australia	AU	220.152.112.0	220.152.119.255
103.25.164.0/24	AS134109	IHIPL-AS-AP	IMS	BD	103.25.164.0	103.25.164.255
123.253.0.0/16	AS4812	CHINANET-SH-AP	China	CN	123.253.0.0	123.253.255.255
123.253.132.0/23	AS17621	CNCGROUP-SH	China	CN	123.253.0.0	123.253.255.255
131.161.8.0/22	AS55967	CNNIC-BAIDU-AP	Beijing	CN	131.161.8.0	131.161.11.255
131.161.8.0/24	AS55967	CNNIC-BAIDU-AP	Beijing	CN	131.161.8.0	131.161.11.255
131.161.9.0/24	AS55967	CNNIC-BAIDU-AP	Beijing	CN	131.161.8.0	131.161.11.255
131.161.10.0/24	AS55967	CNNIC-BAIDU-AP	Beijing	CN	131.161.8.0	131.161.11.255
131.161.11.0/24	AS55967	CNNIC-BAIDU-AP	Beijing	CN	131.161.8.0	131.161.11.255
202.94.1.0/24	AS4808	CHINA169-BJ	China	CN	202.94.0.0	202.94.31.255
43.251.20.0/22	AS9381	WTT-AS-AP	WTT	HK	43.251.20.0	43.251.23.255
103.85.188.0/22	AS132839	POWERLINE-AS-AP	POWER	HK	103.85.188.0	103.85.191.255
103.249.32.0/22	AS9381	WTT-AS-AP	WTT	HK	103.254.116.0	103.254.119.255
103.254.116.0/22	AS9381	WTT-AS-AP	WTT	HK	103.254.116.0	103.254.119.255
173.249.188.0/24	AS55480	ISERVICES-HK	I-Services	HK	173.249.160.0	173.249.191.255
192.67.161.0/24	AS55480	ISERVICES-HK	I-Services	HK	192.67.160.0	192.67.163.255
102.6.204.0/23	AS58503	PUSATMEDIA-AS-ID	PT	ID	102.0.0.0	102.135.255.255
102.6.206.0/23	AS58503	PUSATMEDIA-AS-ID	PT	ID	102.0.0.0	102.135.255.255
116.199.200.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.201.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.202.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.203.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.204.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.205.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.206.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255
116.199.207.0/24	AS38521	PISHON-AS-ID	Pishon	ID	116.199.200.0	116.199.207.255

Bogons

43.251.84.0/22	AS133676	PNPL-AS	Precious	IN	43.251.84.0	43.251.87.255
43.251.84.0/23	AS133676	PNPL-AS	Precious	IN	43.251.84.0	43.251.87.255
103.5.218.0/24	AS17762	HTIL-TTML-IN-AP	Tata	IN	103.5.216.0	103.5.219.255
103.38.8.0/24	AS133295	WEBWERKS-AS	Web	IN	103.38.8.0	103.38.8.255
103.49.236.0/22	AS133715	YPT-AS	YPT	IN	103.49.236.0	103.49.239.255
103.66.168.0/24	AS135719	LMES-AS	Lm	IN	103.66.168.0	103.66.169.255
103.68.84.0/22	AS133676	PNPL-AS	Precious	IN	103.68.84.0	103.68.87.255
103.68.86.0/24	AS133676	PNPL-AS	Precious	IN	103.68.84.0	103.68.87.255
103.69.200.0/24	AS135257	DLGTPL-AS	DL	IN	103.69.200.0	103.69.203.255
103.73.216.0/22	AS133987	PRACHAR-AS	Pracharnama	IN	103.73.216.0	103.73.219.255
103.78.187.0/24	AS134302	WISPL-AS	Wizone	IN	103.78.186.0	103.78.187.255
103.79.236.0/24	AS135870	EXCELPL-AS	Excel	IN	103.79.236.0	103.79.239.255
103.79.237.0/24	AS135870	EXCELPL-AS	Excel	IN	103.79.236.0	103.79.239.255
103.81.103.0/24	AS135850	NSNPLMRJ-AS	Net	IN	103.81.103.0	103.81.103.255
103.197.76.0/24	AS17917	QTLTELECOM-AS-AP	Quadrant	IN	103.197.76.0	103.197.79.255
103.229.232.0/22	AS133676	PNPL-AS	Precious	IN	103.229.232.0	103.229.235.255
103.229.232.0/24	AS18002	WORLDPHONE-IN	AS	IN	103.229.232.0	103.229.235.255
103.229.235.0/24	AS133676	PNPL-AS	Precious	IN	103.229.232.0	103.229.235.255
103.243.8.0/22	AS133676	PNPL-AS	Precious	IN	103.243.8.0	103.243.11.255
202.140.139.0/24	AS9583	SIFY-AS-IN	Sify	IN	202.140.136.0	202.140.139.255
202.181.4.0/24	AS134848	DATACONNECT-AS-IN	Data	IN	202.181.4.0	202.181.7.255
103.43.60.0/22	AS10021	KVH	KVH	JP	103.43.60.0	103.43.63.255
103.227.104.0/22	AS10021	KVH	KVH	JP	103.227.104.0	103.227.107.255
103.252.180.0/22	AS2519	VECTANT	ARTERIA	JP	103.252.180.0	103.252.183.255
202.8.106.0/24	AS9530	SHINSEGAE-AS	SHINSEGAE	KR	202.8.96.0	202.8.127.255
202.158.251.0/24	AS9255	CONNECTPLUS-AS	Singapore	SG	202.158.248.0	202.158.251.255
103.251.71.0/24	AS132900	TSIC-AS-AP	Thai	TH	103.251.71.0	103.251.71.255

Source: www.cidr-report.org

Bogons from Thailand

Bogon Prefix	Origin AS	AS Description	Unallocated Block
103.251.71.0/24	AS132900	TSIC-AS-AP Thai System Integration Co.,Ltd, TH	103.251.71.0 - 103.251.71.255

Bogon ASN		Peer ASN	AS Description
AS56096	Announced by	AS45455	TH-2S1N-AP Two S One N Co Ltd, Internet Service Provider and IT Solutions, TH
AS133528	Announced by	AS9931	CAT-AP The Communication Authoity of Thailand, CAT, TH
AS45606	Announced by	AS45328	NIPA-AS-TH NIPA TECHNOLOGY CO., LTD, TH

Source: www.cidr-report.org

Tools to Help

- Prefix and AS-PATH filtering
- RPKI validator, IRR toolset, IRRPT, BGPQ3
- BGPSEC is standardized

But…

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.

We Are In This Together

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.

The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common routing threats

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.

MANRS

MANRS Actions

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in common routing databases

Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate

Filtering

Filtering – Preventing 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 applies due diligence when checking the correctness of its customer’s announcements, specifically that the customer legitimately holds the ASN and the address space it announces.

In an ideal world, there would be filters on all BGP sessions that only allow prefixes and AS paths that are actually supposed to come in over that BGP session.

Filtering

So it’s absolutely critical that ISPs carefully filter prefixes they receive from their customers. A simple prefix list that allows the prefixes held by the customer (and the customer’s customers) will do the trick:

```
!
ip prefix-list customer-a seq 5 permit 10.0.0.0/8 le 32
ip prefix-list customer-a seq 10 permit 172.16.0.0/12 le 32
ip prefix-list customer-a seq 15 permit 192.168.0.0/16 le 32
!
router bgp 65000
neighbor 192.0.2.2 remote-as 65001
neighbor 192.0.2.2 prefix-list customer-a in
!
```

Filtering

In addition to filtering prefixes, it's a good idea to also filter AS paths. That way, if one filter doesn't work, the other will still make sure only the right prefixes are propagated. Here, a customer with AS 65001 has two customers of their own: ASes 65002 and 65003:

```
!
ip as-path access-list 3 permit ^(65001_)+$
ip as-path access-list 3 permit ^(65001_)+(65002_)+$
ip as-path access-list 3 permit ^(65001_)+(65003_)+$
!
router bgp 65000
neighbor 192.0.2.2 remote-as 65001
neighbor 192.0.2.2 filter-list 3 in
!
```

Filtering

Using the IRR (Internet Routing Registry**) to produce prefix filters**

There is an easy solution to this problem, however. A tool called *bgpq3* exists which automates all this for you.

```
# bgpq3 -4 -l Customer-A-v4 AS13558
no ip prefix-list Customer-A-v4
ip prefix-list Customer-A-v4 permit 146.145.118.0/24
ip prefix-list Customer-A-v4 permit 198.232.133.0/24

# bgpq3 -4 -Jl Customer-A-v4 AS13558
policy-options {
replace:
 prefix-list Customer-A-v4 {
    146.145.118.0/24;
    198.232.133.0/24;
 }
}
```

https://github.com/snar/bgpq3
http://www.irr.net/docs/list.html

Anti Spoofing

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 incorrect source IP address from entering and leaving the network.

There are various techniques you can implement SAV

- uRPF (Unicast Reverse Path Forwarding)
  - uRPF prevents spoofing attacks. Whenever your router receives an IP packet it will check if it has a **matching entry in the routing table for the source IP address**. If it doesn't match, the packet will be discarded. uRPF has two modes Strict and Loose.
- Access Control List (ACLs)

Anti Spoofing

Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Spoof Private	Spoof Routable	Adjacency Spoofing
461062	2018-05-08 11:09:16	49.231.180.x/24	45458 (SBN-AWN-AS-02-AP)	tha (Thailand)	no	received	received	/8
453942	2018-04-27 03:42:57	49.231.180.x/24	45458 (SBN-AWN-AS-02-AP)	tha (Thailand)	no	received	received	/8
453291	2018-04-26 07:04:32	49.231.180.x/24	45458 (SBN-AWN-AS-02-AP)	tha (Thailand)	no	received	received	/8
443994	2018-04-11 15:36:58	2403:6200:88xx::/40	45629 (JASTEL-NETWORK-TH-AP)	tha (Thailand)	no	blocked	received	/16
442846	2018-04-10 00:12:34	2403:6200:88xx::/40	45629 (JASTEL-NETWORK-TH-AP)	tha (Thailand)	no	blocked	received	/16
441993	2018-04-08 14:11:14	2403:6200:88xx::/40	45629 (JASTEL-NETWORK-TH-AP)	tha (Thailand)	no	blocked	received	/16
440880	2018-04-06 12:52:02	2403:6200:88xx::/40	45629 (JASTEL-NETWORK-TH-AP)	tha (Thailand)	no	blocked	received	/16
440211	2018-04-05 11:05:50	2403:6200:88xx::/40	45629 (JASTEL-NETWORK-TH-AP)	tha (Thailand)	no	blocked	received	/16
426142	2018-03-13 12:24:53	171.100.31.x/24	7470 (TRUEINTERNET-AS-AP)	tha (Thailand)	yes	received	received	/8
417129	2018-02-26 11:14:37	49.231.180.x/24	45458 (SBN-AWN-AS-02-AP)	tha (Thailand)	no	received	received	/8
406508	2018-02-08 05:21:36	49.231.44.x/24	45430 (SBN-AWN-IIG-AS-AP)	tha (Thailand)	no	received	received	/8
387730	2018-01-09 14:56:41	122.154.104.x/24	9931 (CAT-AP)	tha (Thailand)	yes	blocked	received	/8
387698	2018-01-09 14:10:06	122.154.104.x/24	9931 (CAT-AP)	tha (Thailand)	yes	blocked	received	/8
387593	2018-01-09 10:59:32	122.154.104.x/24	9931 (CAT-AP)	tha (Thailand)	yes	blocked	received	/8
384537	2018-01-04 07:38:12	49.231.94.x/24	45458 (SBN-AWN-AS-02-AP)	tha (Thailand)	no	received	received	none
384531	2018-01-04 07:30:59	49.231.195.x/24	45458 (SBN-AWN-AS-02-AP)	tha (Thailand)	no	received	received	none

https://spoofer.caida.org/recent_tests.php?country_include=tha

Coordination

Publicly accessible and up-to-date contact information is essential to promoting communication and collaboration between network operators. Network operators are advised to maintain their contact data on objects registered in RIR whois databases such as APNIC and also on their public website.

```
aut-num:        AS133585
as-name:        PPS-AS-AP
descr:          PON Project Services Pty Ltd
country:        AU
org:            ORG-PPSP1-AP
admin-c:        PPSP1-AP
tech-c:         PPSP1-AP
mnt-by:         MAINT-PPS-AU
mnt-irt:        IRT-PPS-AU
mnt-routes:     MAINT-PPS-AU
last-modified:  2017-10-16T00:28:06Z
source:         APNIC
```

```
irt:            IRT-PPS-AU
address:        2a/5-7 Anella Av, Castle Hill NSW 2153
e-mail:         ats@ponprojects.com
abuse-mailbox:  ats@ponprojects.com
admin-c:        PPSP1-AP
tech-c:         PPSP1-AP
auth:           # Filtered
mnt-by:         MAINT-PPS-AU
last-modified:  2018-03-07T12:42:51Z
source:         APNIC
```

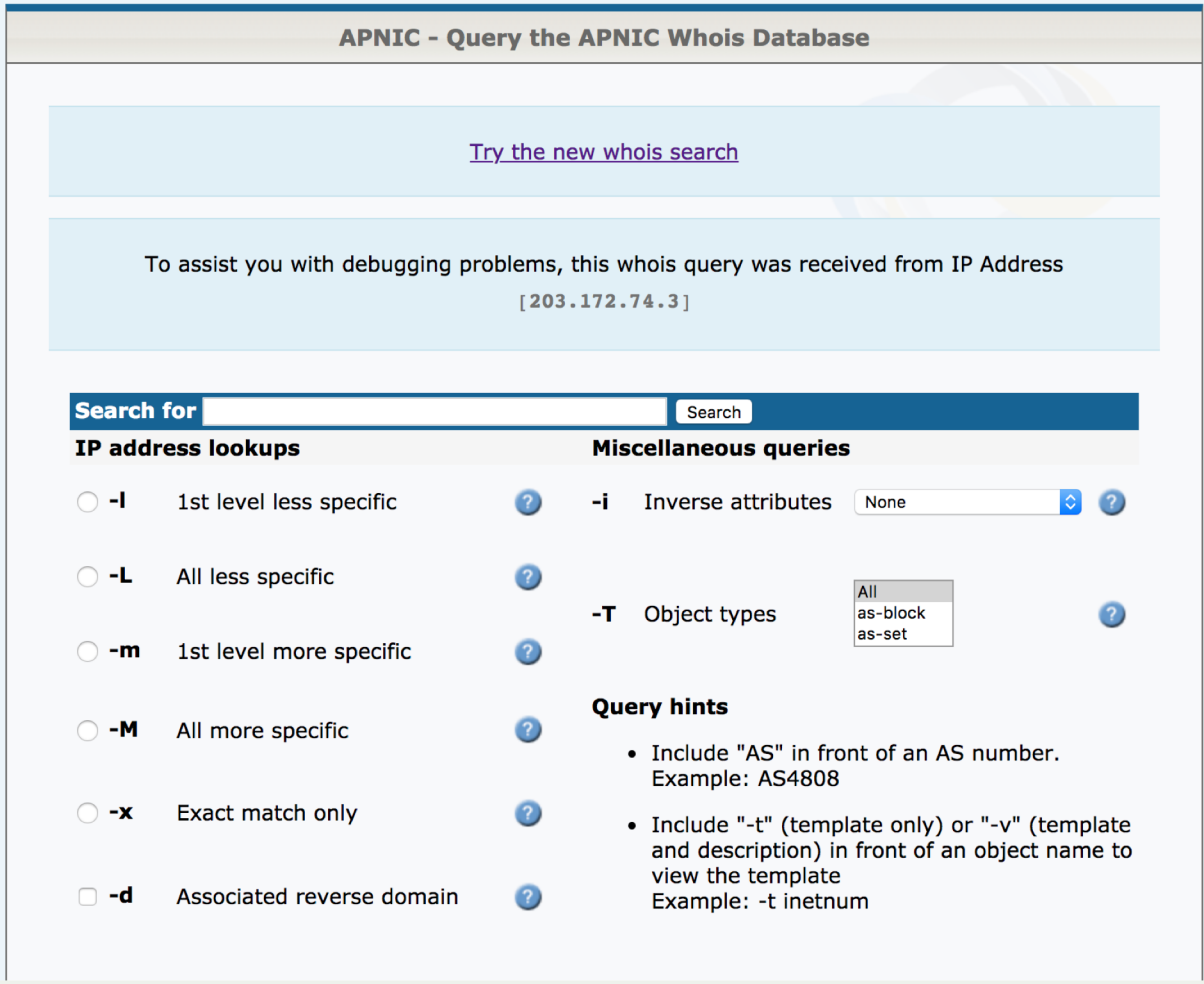
Coordination

The APNIC Whois Database, stores information as ‘Objects’. Objects can store information about:

- IP address ranges
- Routing policies
- Reverse DNS delegations
- Network contact information.

Numeric Internet resources must be properly and accurately registered in the APNIC whois Database to fulfil the goals of global addressing policy.

$ whois -h whois.apnic.net AS133585



Coordination

Maintain Contact Information in PeeringDB

The PeeringDB (https://www.peeringdb.com) is an open resource for networks to share their peering information and other relevant information amongst each other. Networks are responsible for maintaining their records in the database. Having a PeeringDB record allows you to consolidate your network information in a single location, and as an operator, allows you to research other networks and obtain additional information such as links to an operator's looking glass, what facilities they peer in, contact information, etc.

Global Validation

Relevant MANRS expected and advanced actions:

- Network operator is able to communicate to their adjacent networks which announcements are correct;
- Network operator has publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties.

Routing information should be made available on a global scale to facilitate validation, which includes routing policy, ASNs and prefixes that are intended to be advertised to third parties. Since the extent of the internet is global, information should be made public and published in a well known place using a common format.

Global Validation

MANRS participants should maintain updated public information in order to facilitate the validation of routing information. This includes the following data:

Object	Source	Description
aut-num	IRR	Policy documentation
route/route6	IRR	NLRI/origin
as-set	IRR	Customer cone
ROA	RPKI	NLRI/origin

Global Validation

Providing information through the RPKI system

Resource Public Key Infrastructure (RPKI) is a public key infrastructure framework designed to secure the Internet's routing infrastructure, specifically the Border Gateway Protocol. RPKI provides a way to connect Internet number resource information (such as IP Addresses) to a trust anchor.

The RPKI repository can store information about prefixes originated by your network in the form of Route Origin Authorization (ROA) objects. Note, that these do not include your customer announcements, but only prefixes that belong to your ASN. Only the origin ASN is verified, not the full path.

Global Validation

A ROA or Route Origin Authorization is an attestation of a BGP route announcement. It attests that the origin AS number is authorized to announce the prefix(es). The attestation can be verified cryptographically using RPKI.

49.0.89.0/24	AIS Fibre
49.0.90.0/24	AIS Fibre
49.0.91.0/24	AIS Fibre
49.0.92.0/24	AIS Fibre
49.0.93.0/24	AIS Fibre
49.0.94.0/24	AIS Fibre
49.0.95.0/24	AIS Fibre
49.228.0.0/18	408/60 PHP Bld. 15th Fl Phaholyothin Rd Samsen Nai Phayathai
49.228.0.0/24	AIS Fibre
49.228.1.0/24	AIS Fibre
49.228.2.0/24	AIS Fibre
49.228.3.0/24	AIS Fibre
49.228.8.0/22	AIS Fibre
49.228.12.0/24	AIS Fibre
49.228.14.0/24	AIS Fibre
49.228.15.0/24	AIS Fibre

https://bgp.he.net/AS133481#_prefixes

Benefits of Improved Routing Security

Signals an organization's security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships.

Heads off routing incidents, helping networks readily identify and address problems with customers or peers.

Improves a network's operational efficiency by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.

Implementing best practices alleviates many routing concerns of security-focused enterprises and other customers.

Everyone Benefits

Joining MANRS means joining a community of security-minded network operators committed to making the global routing infrastructure more robust and secure.

Consistent MANRS adoption yields steady improvement, but we need more networks to implement the actions and more customers to demand routing security best practices.

The more network operators apply MANRS actions, the fewer incidents there will be, and the less damage they can do.

MANRS is an Important Step

Security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet.

MANRS is the minimum an operator should consider, with low risk and cost-effective actions.

MANRS is not a one-stop solution to all of the Internet's routing woes, but it is an important step toward a globally robust and secure routing infrastructure.

Why join MANRS?

- Improve your security posture and reduce the number and impact of routing incidents
- Join a community of security-minded operators working together to make the Internet better
- Use MANRS as a competitive differentiator

Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives

MANRS Implementation Guide

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- https://www.manrs.org/bcop/

Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017

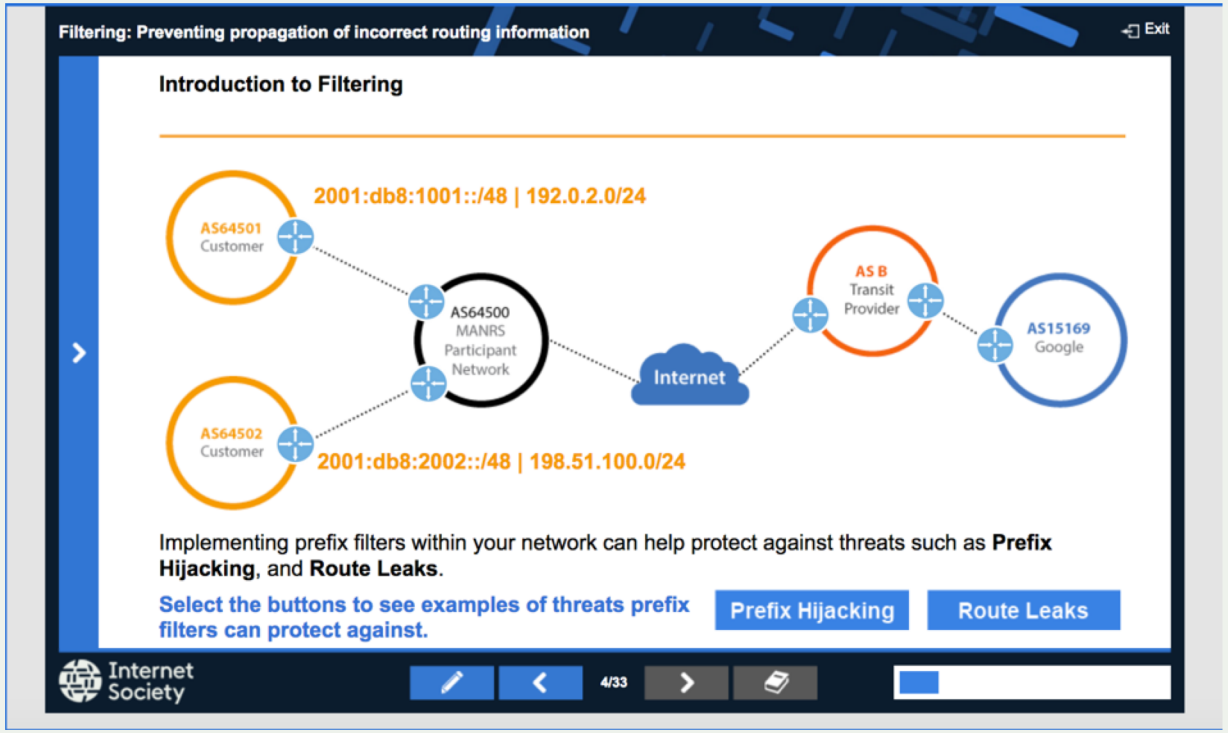
MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

https://www.manrs.org/tutorials



Thank you.

Aftab Siddiqui

siddiqui@isoc.org

manrs.org