ICANN

Using BGP & DNS to Rob You Blind

SSAC | ICANN62 | June 2018

Security and Stability Advisory Committee (SSAC)

Who We Are

- 37 Members
- Appointed by the ICANN Board

What We Do

Charter: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)

How We Advise

101 Publications since 2002

REPORTS ADVISORIES COMMENTS

OUTREACH

Agenda

1 Introductions

2 What is BGP and what are BGP hijacks?

3 The Amazon Route53 Attack

4 Detection and Mitigation

5 Relevant SSAC Publications

6 What you can do to help

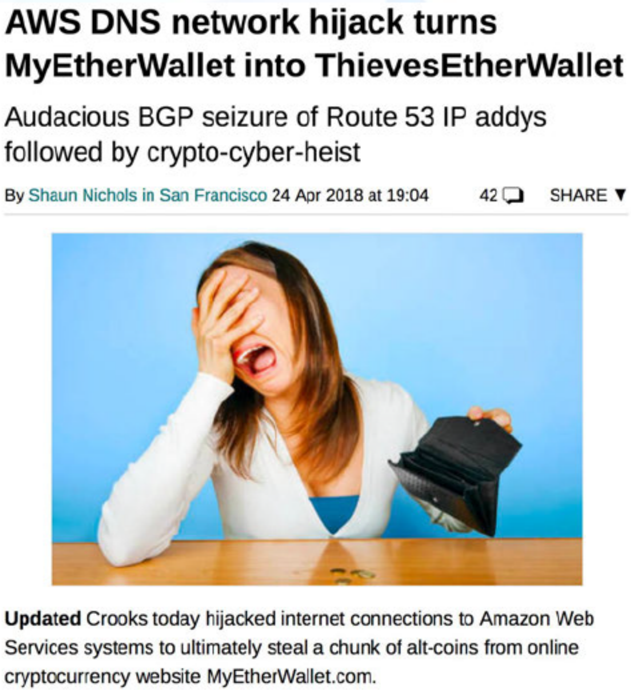
Introduction

Introductions

- Panel/presenters
  - Cristian Hesselman
  - Merike Kaeo
  - Warren Kumari
  - Danny McPherson
  - Rod Rasmussen

Disturbing new twist on an old attack method

The Register's Coverage:



AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

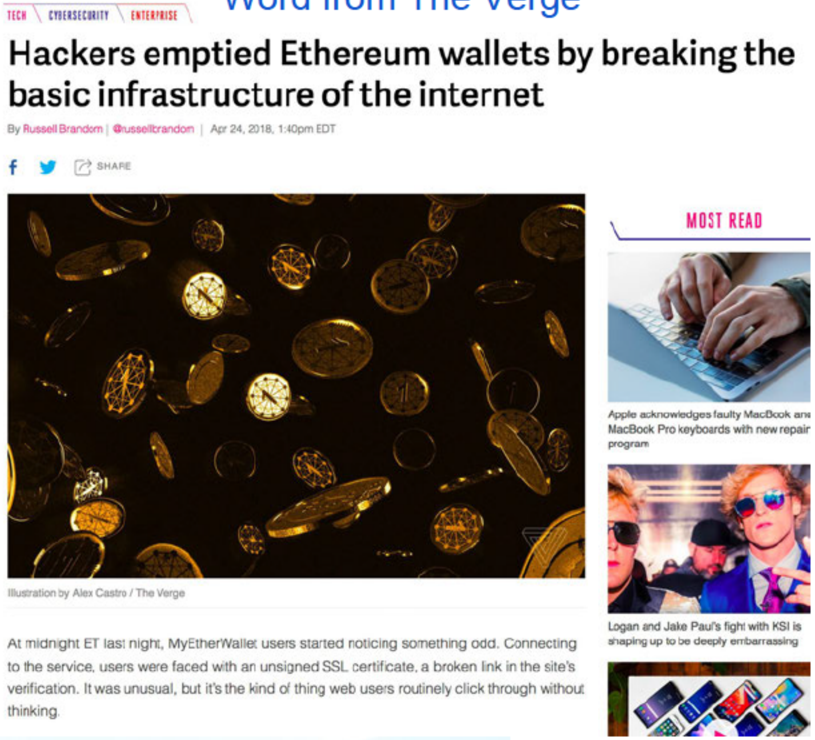
Audacious BGP seizure of Route 53 IP addys followed by crypto-cyber-heist

By Shaun Nichols in San Francisco 24 Apr 2018 at 19:04 42 SHARE ▼

Updated Crooks today hijacked internet connections to Amazon Web Services systems to ultimately steal a chunk of alt-coins from online cryptocurrency website MyEtherWallet.com.

https://www.theregister.co.uk/2018/04/24/myetherwallet_dns_hijack

Word from The Verge



Hackers emptied Ethereum wallets by breaking the basic infrastructure of the internet

By Russell Brandom | @russellbrandom | Apr 24, 2018, 1:40pm EDT

Illustration by Alex Castro / The Verge

At midnight ET last night, MyEtherWallet users started noticing something odd. Connecting to the service, users were faced with an unsigned SSL certificate, a broken link in the site's verification. It was unusual, but it's the kind of thing web users routinely click through without thinking.

Apple acknowledges faulty MacBook and MacBook Pro keyboards with new repair program

Logan and Jake Paul's fight with KSI is shaping up to be deeply embarrassing

https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum

Abusing BGP for fun & profit

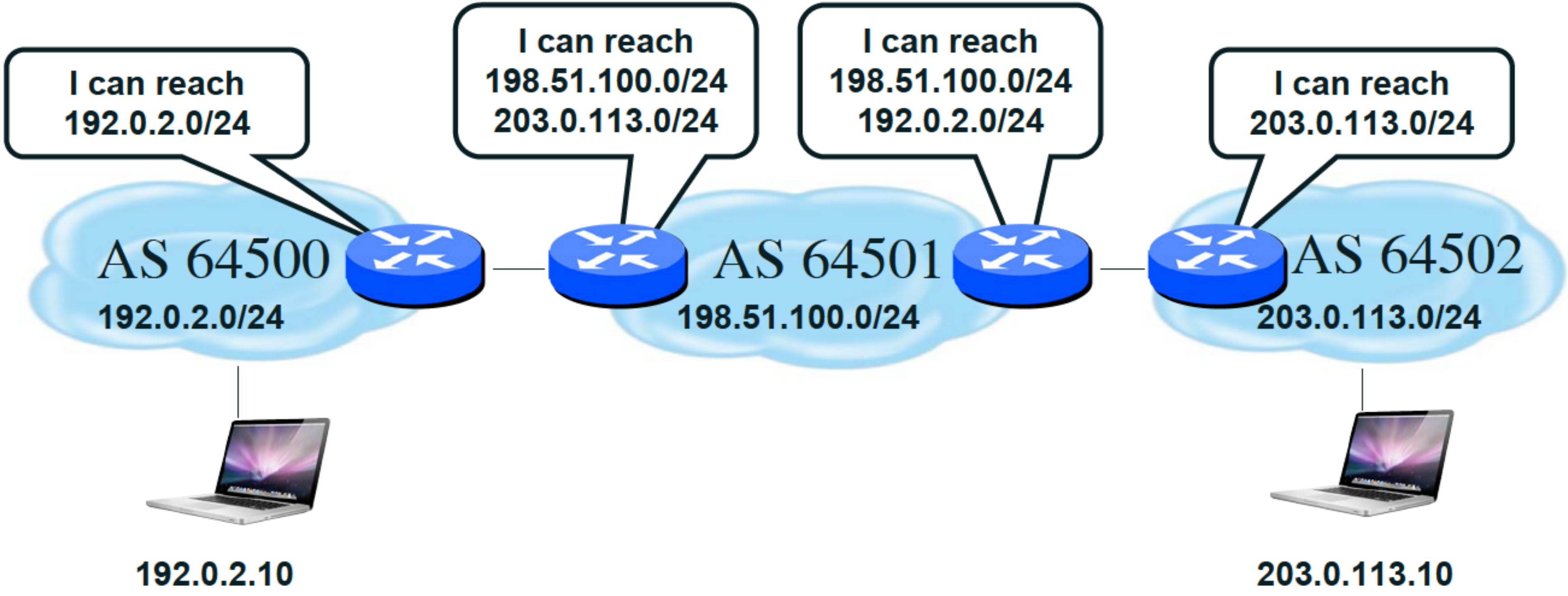
- Cybercrooks created fake “MyEtherWallet” website to steal user logins
- MyEtherWallet is a cryptocurrency wallet service for storing your Ethereum
- In a short time, siphoned $170K from users by re-using their login info in real time.
- Never hacked actual site or sent out lures
- Used attack against underlying DNS service to point users to fake site
- THAT attack utilized a BGP routing attack that substituted fake information into the global routing tables for a chunk of Amazon’s Auth DNS service
- Attack affected potentially thousands of domains, but target appears to just be the one domain and website
- Users redirected without much warning since the underlying infrastructure was changed
- Hard to detect and mitigate since neither company was attacked directly

What is BGP?

What is BGP?

- Border Gateway Protocol
  - Used to route traffic via loosely interconnected networks
- Each network is identified via a unique autonomous system (AS) number
- Each AS asserts reachability for the destination to which it provides connectivity
- No central authority or point of control
  - Highly resilient and provides complete autonomy at the network layer, but also prone to both errors and attacks
- RIRs/NIRs allocate IP address blocks but do NOT have operational role

BGP in Action



What is a BGP hijack?

What is a BGP Hijack?

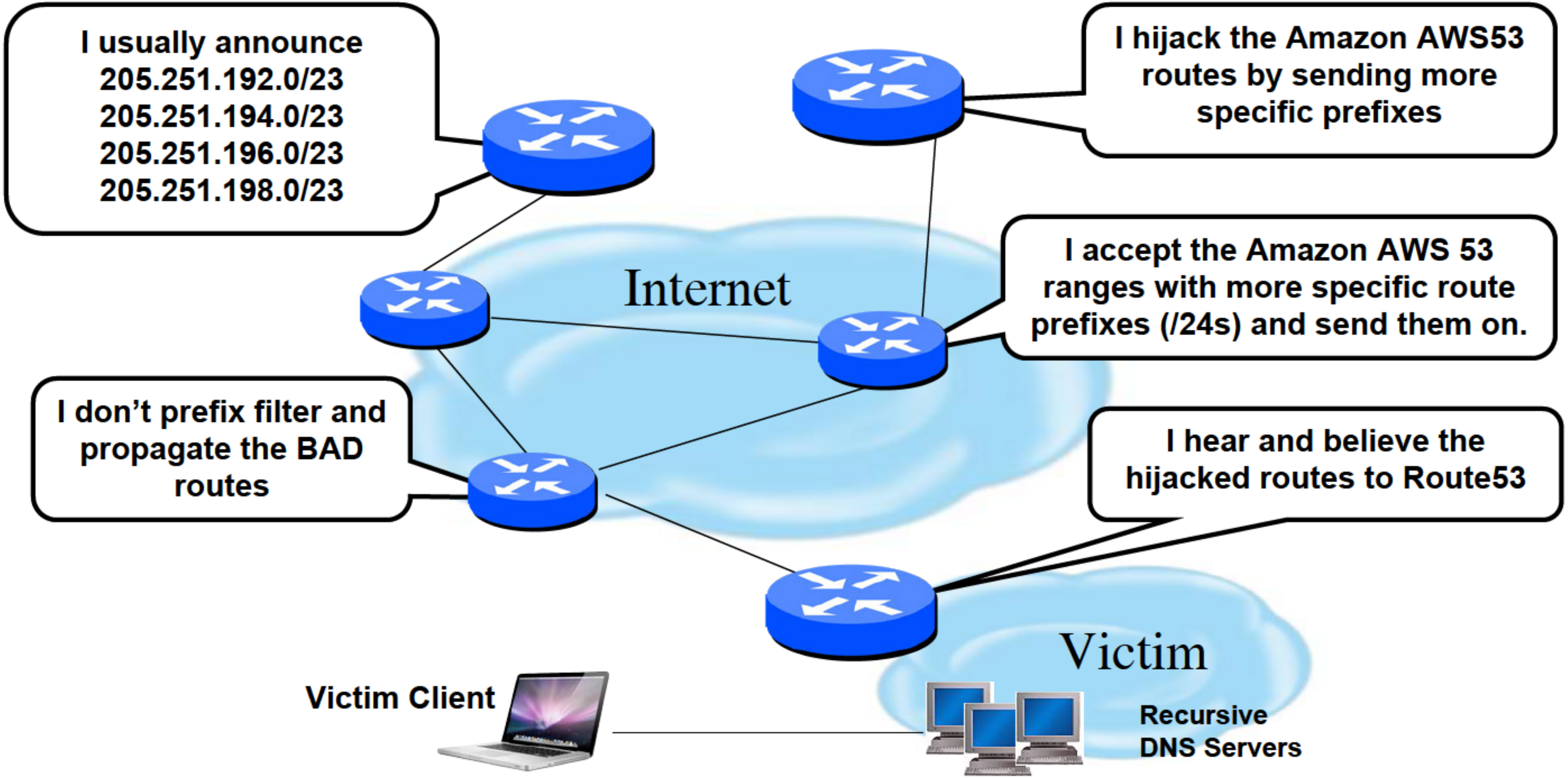
- BGP works under a series of rules to determine the most optimal route
  - The longest prefix match is always preferred
  - Example: 192.0.2.0/24 will always be preferred over 192.0.2.0/23
- To be good Internet citizens, aggregating routes is considered good practice
  - Route aggregation is necessary to fit the Internet’s routing table in router memory
- BGP hijacking occurs when an **illegitimate** route is advertised and preferred instead of a legitimate route
- BGP hijacks can be malicious or unintentional configuration mistakes

The Amazon Route53 Attack

DNS Compromise due to Route Hijack

- Amazon route prefixes were hijacked
- Amazon's Route53 DNS traffic was re-routed to malicious DNS server
- The malicious DNS authoritative server had a legitimate IP address
- Any query to DNS resolvers that asked for names handled by Route53 would route to malicious DNS authoritative servers
- These servers sent answers back to DNS resolvers to have the originating client send traffic to malicious sites
- Essentially a DNS cache poisoning attack

Route Hijack and DNS Consequences



I usually announce
205.251.192.0/23
205.251.194.0/23
205.251.196.0/23
205.251.198.0/23

I hijack the Amazon AWS53 routes by sending more specific prefixes

I accept the Amazon AWS 53 ranges with more specific route prefixes (/24s) and send them on.

I don't prefix filter and propagate the BAD routes

I hear and believe the hijacked routes to Route53

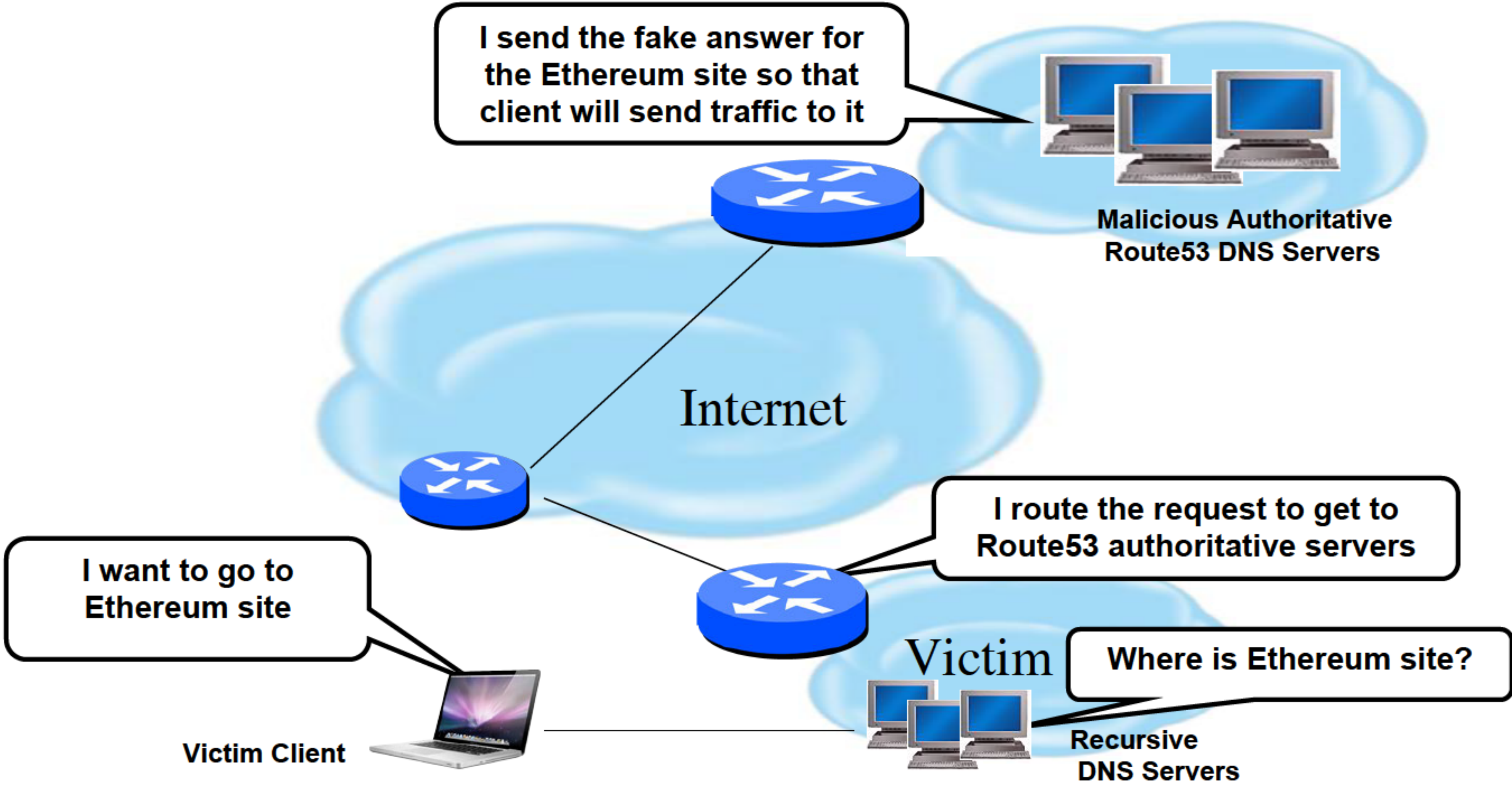
Internet

Victim

Victim Client

Recursive
DNS Servers

Route Hijack and DNS Consequences



I send the fake answer for the Ethereum site so that client will send traffic to it
Malicious Authoritative Route53 DNS Servers
Internet
I route the request to get to Route53 authoritative servers
I want to go to Ethereum site
Victim
Where is Ethereum site?
Victim Client
Recursive DNS Servers

What else can be done using this attack?

- Pharming
- Email interception
- Access credential theft
- Intelligence on who talks to targeted networks/domains
- Others…

Detection and Mitigation

Detection

- BGP Stream (twitter.com/bgpstream)
- Bgpmon.net, www.thousandeyes.com
- DNS resolution monitoring services
- Sudden drops in traffic / requests
- Canaries using RIPE Atlas (https://atlas.ripe.net/) or other tools

Mitigation Techniques (Routing)

- BGP Prefix filtering
- Mutually Agreed Norms for Routing Security (MANRS) www.manrs.org
    - unicast Reverse Path Forwarding (uRPF)
    - BGP prefix filtering
    - Resource Public Key Infrastructure (RPKI)
- Use longest prefix possible for critical infrastructure

Mitigation Techniques (DNS & Web)

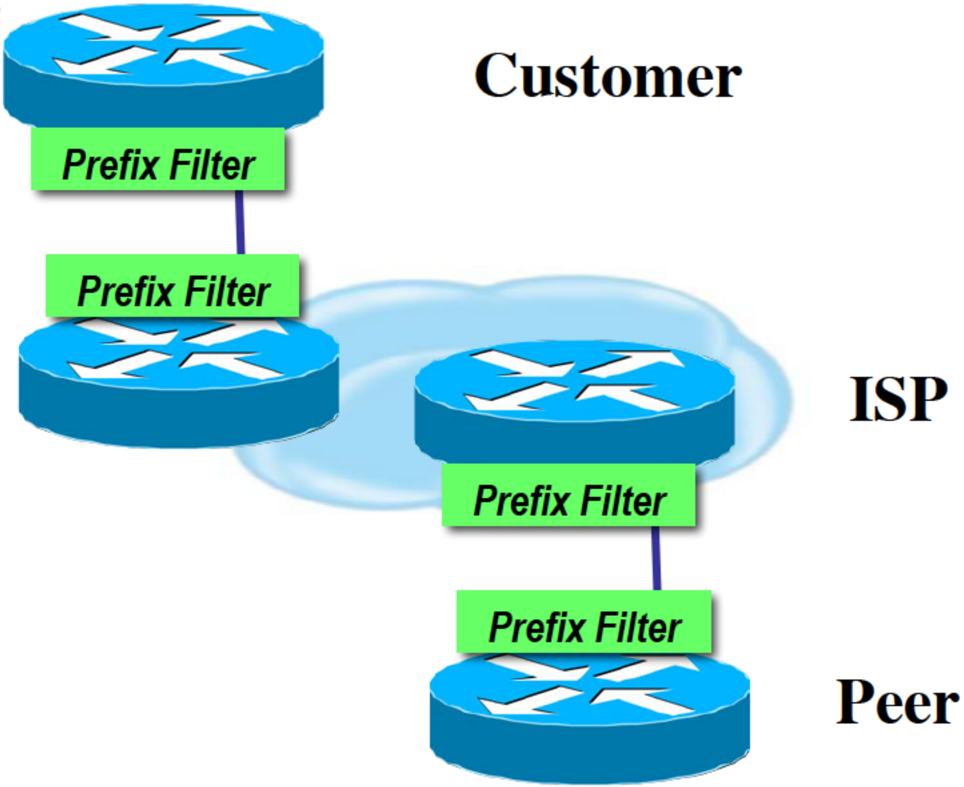
- For the DNS
  - Resiliency
    - Multiple Autonomous Systems (AS)
    - Multiple providers - take care regarding independence
    - External provider and on-premises DNS services
    - Monitor traffic volume for unexpected changes - including reduced volume
  - DNSSEC
    - Signing
    - Validation
- For the Web
  - DANE for HTTPS
  - HTTPS X.509 certificates (Hopefully users don’t just ignore warnings and click through!)

BGP Prefix Filtering

- All BGP Prefixes coming into your network and leaving your network need to be filtered to enforce a policy.
- The problem is many ISPs are not:
  - Filtering Comprehensively
  - Filtering their customer’s prefixes
  - Filtering prefixes going out of their network.

Where to Prefix Filter ?

- Customer's Ingress/Egress
- ISP Ingress on Customer (may Egress to Customer)
- ISP Egress to Peer and Ingress from Peer
- Peer Ingress from ISP and Egress to ISP



Prefix Filter Bogons and RIR Blocks

- Templates available from the Bogon Project:
  - http://www.cymru.com/Bogons/index.html
- Cisco Template
  - ftp://ftp-eng.cisco.com/cons/isp/security/Ingress-Prefix-Filter-Templates/
- Juniper Template
  - http://www.qorbit.net/documents.html

Resource Public Key Infrastructure (RPKI)

- Allows recipients of route advertisements to validate whether an Autonomous System (AS) is authorized to announce a specific prefix
- Main building blocks are trust anchors, Route Origin Authorizations (ROAs) and validators.
- Operators who originate routes register them by creating a ROA at a trust anchor
  - ROAs specify both a network and its prefix length
  - Trust anchors used today are the RIRs (LACNIC, APNIC, ARIN, RIPE, AFRINIC)
- Operators who receive route advertisements can validate the advertisements with RPKI

RFC2827 (BCP38) – Ingress Filtering

- If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

Audit and Validate Your Routing Infrastructures

- Are appropriate paths used?
  - check routing tables
  - verify configurations
- Is a router compromised?
  - check access logs

Relevant SSAC Publications

Relevant SSAC Publications

- https://www.icann.org/groups/ssac/documents
- SAC004: Securing the Edge (17 October 2002)
- SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
- SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
- SAC049: SSAC Report on DNS Zone Risk Assessment and Management (03 June 2011)
- SAC075: SSAC Comments to ITU-D on Establishing New Certification Authorities (03 December 2015)

What you can do to help

What You Can Do to Help

- Socialize good routing and BGP practices
  - MANRS (including RPKI)
  - BGP Prefix Filtering
- DNSSEC sign your zones
- Perform DNSSEC validation
- DNS resolution monitoring
- Monitor incoming traffic
- Understand your routing environment and provision with hijacking in-mind
- Multi-home authoritative DNS servers using differing ASNs
- Add Internet Health as a consideration of your network provisioning decisions
- Actively monitor prefixes used for DNS infrastructure to spot hijacks early on
- Help management understand potential effects of poor routing hygiene on business continuity

Panel Discussion / Q&A

Thank you