Make BGP Great Again

BY JAMES HEMMINGS

ABERTAY UNIVERSITY

$Whoami

- 3rd Year Ethical Hacking Student.
- Former US Volunteer Firefighter/EMT.

- **Interests**
- National security
- Critical national infrastructure (SCADA)
- Offensive capabilities (Red Teaming + Pentesting)
- Linux

Agenda

- BGP History
- BGP Protocol 101
- BGP Hijacking
  - BGP Hijacking In The Wild
  - Attacker motive
  - Attack methods
  - What is BGP Hijacking
- Countermeasures
- Government Strategy
- Conclusion

BGP History

- **June 1989 (RFC 1105) -- (BGP-1)** Initial definition of the BGP protocol, replaced EGP
- **June 1990 (RFC 1163) -- (BGP-2)** Removed directional topology, BGP 1 issues resolved
- **October 1991 (RFC 1267) -- (BGP-3)** Optimized, and simplified route information exchange. Identification capability added
- **July 1994 (RFC 1654) -- (BGP-4)** Initial standard created for BGP-4
- **March 1995 (RFC 1771) -- (BGP-4)** CIDR support, allows prefixes to be specified to represent aggregated networks, other tweaks

BGP – Border Gateway Protocol

- Critical to the internet backbone, used extensively around the world
  - Very old protocol
- Exchanges routing information between Autonomous Systems (AS)
- Used to determine, and exchange path information between ISP’s
- Announces IP prefixes available within an AS
- Trust by default – routes not usually verified

BGP Operations 101

- 1) Establishes session using TCP Port 179 to neighbour
- 2) Exchanges all active routes within BGP
- 3) Exchanges incremental updates. (Using route UPDATE messages)

- **KEEPALIVE** messages sent for duration of communication.
- **NOTIFICATION** messages sent in response to error or special conditions

Regional Internet Registries

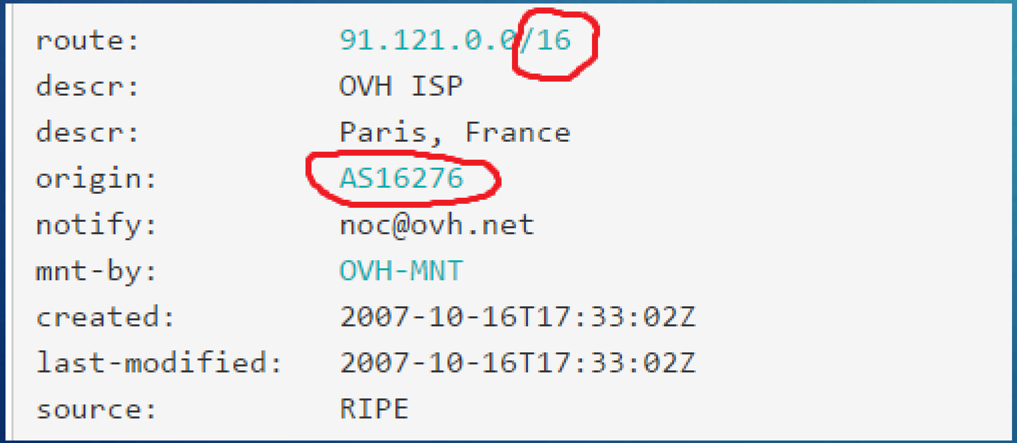
- Non-profits corporations, manage and register Internet Protocol address's and Autonomous Systems numbers per region
  - No association between ASN and IP, except for RIPE

- RIPE NCC – Europe, Middle East and Central Asia
- LACNIC – Latin America, portions of the Caribbean
- ARIN – Canada, Caribbean, North Atlantic Islands, and the United States
- APNIC – Portions of Asia, and portions of Oceania
- AFRINIC – Africa, portions of Indian Ocean

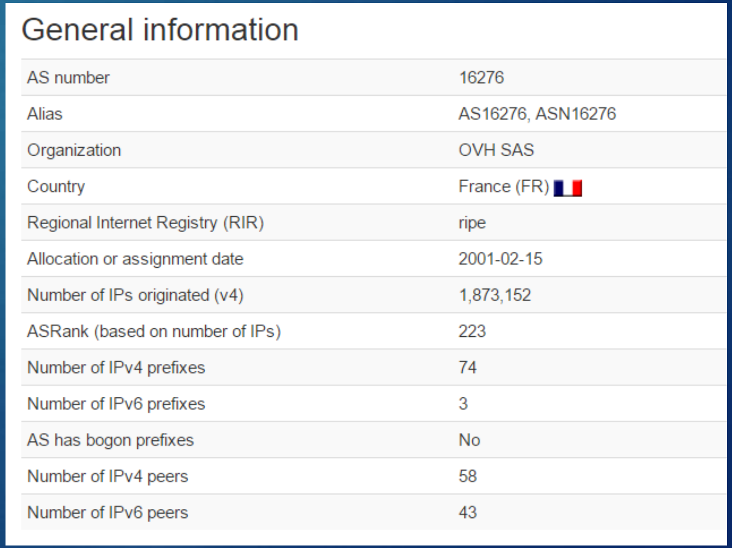
Autonomous Systems (AS)

- Collection of IP prefixes under the control of one or more operators, on behalf of a organization that presents clearly defined routing policy to the internet.

- ASN's assigned by RIPE, LACNIC, ARIN, APNIC, AFRINIC ect. (Depending on region).



```
route:          91.121.0.0/16
descr:          OVH ISP
descr:          Paris, France
origin:         AS16276
notify:         noc@ovh.net
mnt-by:         OVH-MNT
created:        2007-10-16T17:33:02Z
last-modified:  2007-10-16T17:33:02Z
source:         RIPE
```



General information

AS number	16276
Alias	AS16276, ASN16276
Organization	OVH SAS
Country	France (FR) 🇫🇷
Regional Internet Registry (RIR)	ripe
Allocation or assignment date	2001-02-15
Number of IPs originated (v4)	1,873,152
ASRank (based on number of IPs)	223
Number of IPv4 prefixes	74
Number of IPv6 prefixes	3
AS has bogon prefixes	No
Number of IPv4 peers	58
Number of IPv6 peers	43

BGP Attributes

- **AS Path:** Sequence of ASes a route has traversed.
  - Used for loop detection, and path metrics.
- **Local Pref:** Advertises to IBGP neighbour's on how to leave the network (Outbound traffic only).
  - Used for route selection. Highest path value wins.
- **Community:** Tagging technique to mark routes, used to apply routing policies within a network.
- **Origin:** Informs AS's were the prefix was originally originated from.
- **Multi Exit Discriminator:** Advertises to EBGP neighbour's on how to exit the AS to reach networks owned by this AS (Incoming traffic)
- **Next Hop:** Next hop IP address to reach the destination network.

BGP Messages

- **OPEN**
  - Negotiate, and establish peering (TCP179)
- **UPDATE**
  - Exchanges routing information (Route updates)
- **KEEPALIVE**
  - Sends continuous messages to maintain peering session
- **NOTIFICATION**
  - Reports errors, causing session reset

BGP Prefixes

- Defines path autonomous systems must transverse to reach announced IPv4 or IPv6 IP blocks (CIDR Block/Network Info)
- Carried within Network Layer Reachability Information (NLRI), within BGP UPDATE messages.
- Example: (IPV4) **701 1239 42** 204.10.12.0/24

BGP Path Selection

- Uses path selection algorithm, assigns various attributes to each path, manipulated to control the path that is selected.
- BGP examines values of BGP attributes in ordered manner, until one route is narrowed down as best path.
- Selection criteria such as: Weight, local preference, network or aggregate, shortest AS_PATH, lowest origin type, lowest MED, EBGP or IBGP, lowest IGP metric, multiple paths, external paths, lowest router ID, minimum cluster list, lowest neighbour address.

Limitations of BGP

- **Integrity**
  - No protection against tampering of data within BGP messages, or that the message has been replayed.
- **Validation**
  - BGP does not validate autonomous system authority to announce a specific network prefix. Path subversion allows attacker to announce as shortest path, even if that is incorrect.
- **Trust**
  - Path attributes sent within BGP are not verified as authentic, attackers can alter path attributes to manipulate core routing infrastructure.

BGP Hijacking In The Wild 1

- **April 2010 – Chinese ISP Hijack**
  - Misconfiguration?? 37,000 unique prefixes affected. China denied it. Affected DOD, Navy, USMC, Airforce and lots of other Ases
- **March 2011 – Facebook BGP Hijack**
  - Chinese network advertised several Facebook prefixes, long and odd AS paths.
- **October 2013 - May 2014 – Canadian Bitcoin Hijack**
  - AS_Path spoofing, Canadian ISP. $83,000 bitcoins stolen.
- **March 2013 – Spamhaus DDoS & BGP Hijack**
  - 300Gbps DDoS (Nearly broke internet). Specific /32 route announced for Spamhaus spam query server. Lots of emails marked as spam.
- **March 2014 – Turkey Censorship Hijack**
  - Global DNS hard null route, propagated outside Turkey. Global outages.

BGP Hijacking In The Wild 2

- **December 2014 – Syrian Telecom BGP Hijack**
  - 1481 prefixes effected, networks such as US DOD, Dell, Akamai, Telefonica, Youtube, Redhat ect ect.
- **February 2016 – Staminus Communications Hijack**
  - Two management IP ranges hijacked by BackConnect LLC, rival DDoS mitigation firm
  - Occurred over two days (20th, 21st)
  - Staminus compromised March 14th

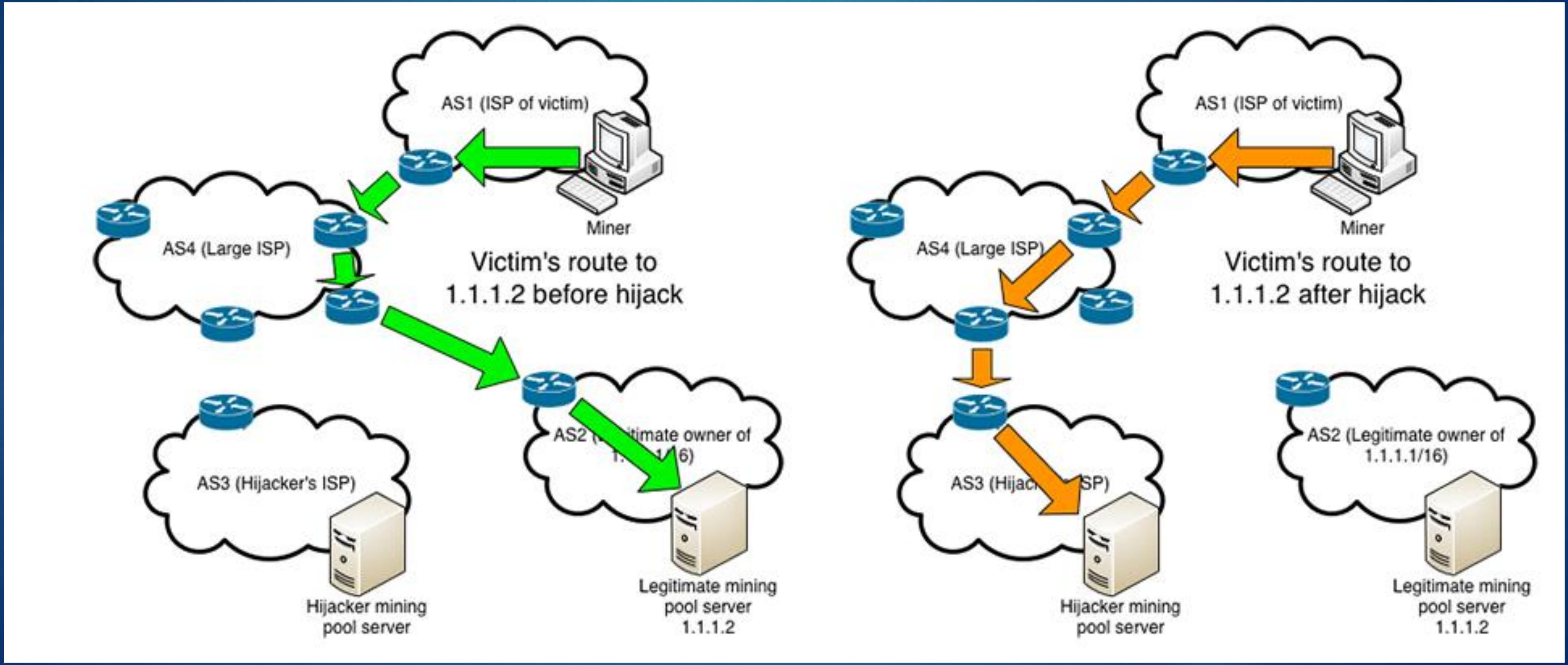
What is BGP Hijacking

- The manipulation of BGP, causing data to be re-routed in an attackers favour which allows for the interception or modification of traffic, and theft of IP prefixes.

- How??
- Announce specific victim IP prefix.
  - Prefix hijacking

- Announce a more specific IP prefix
  - Eg, /15 victim, /24 attacker.
  - Sub-Prefix hijacking

BGP Hijacking Diagram


AS1 (ISP of victim)
Miner
AS4 (Large ISP)
Victim's route to 1.1.1.2 before hijack
AS2 (Legitimate owner of 1.1.1.1/16)
AS3 (Hijacker's ISP)
Hijacker mining pool server
Legitimate mining pool server 1.1.1.2
AS1 (ISP of victim)
Miner
AS4 (Large ISP)
Victim's route to 1.1.1.2 after hijack
AS3 (Hijacker's ISP)
AS2 (Legitimate owner of 1.1.1.1/16)
Hijacker mining pool server
Legitimate mining pool server 1.1.1.2

https://www.bishopfox.com/blog/2015/08/an-overview-of-bgp-hijacking/

Motive

- Malicious activities
  - Spam, advertising, denial of service attacks
- Corporate/Nation State Espionage
  - Perform MITM attacks, steal information and disrupt other networks
  - Reclaim botnets
    - Hacking Team 2015 – Italian Military Police (Special Operations Group)
      - Reclaimed RAT C&C servers using BGP hijacking
- Profit
  - Canadian bitcoin hijack

https://bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/

BGP Prefix Hijacking

- Announcing a legitimate AS prefix without permission
  - This type of attack, can effect local autonomous systems. Could propagate globally depending on policies and best path selection
  - Announce shorter AS path, fool BGP path selection
- Attacker does not own the prefix, or have permission to announce it
- Announces prefix using attackers AS, with victims prefix
  - AS9: 141.212.110.0/24 (Victim)
  - AS1: 141.212.110.0/24 (Attacker)
- Intercept/tamper with data, perform man in the middle attacks

BGP Sub-Prefix Hijacking

- Announcing victim prefix without permission. More specific CIDR notation
  - AS9: 37.42.21.0/15 (Victim)
  - AS1: 37.42.21.0/24 (Attacker)

- Routers will select the attackers path, due to the more specific route
  - Most likely global propagation, depending on filtering

- Intercept/tamper with data, perform man in the middle attacks

Countermeasures … 1

- **Prefix Filtering**
  - Ingress/egress route filtering, prevent bogus route advertisements inbound or outbound.
    - Egress filtering prevents misconfiguration errors on local AS
  - List authorized neighbour prefixes in prefix list
    - Not on prefix list? Rejected
- **Caveats**
  - "Weakest leak in the chain"
    - Everybody must implement this for it to work effectively, or hijacking will still be possible in most cases
    - Most ISPs do not use prefix filtering, due to maintenance upkeep and no legal requirement to implement it

Countermeasures … 1

- **Real Time Monitoring Systems**
  - Monitoring solutions such as BGP Mon, RIPE MyASN, and PHAS are the most recommended solution.
  - Provides detection capability, enabling IT/NOC teams to respond post-hijack within minutes.

  - **Caveats**
  - Does not prevent BGP hijacking
  - Post incident response
  - Some services cost

Countermeasure … 2

- **Resource Public Key Infrastructure (RPKI)**
  - Sign IP prefix, and ASN number using cryptographic signature (RFC6480)
    - Provides some integrity, not the most secure method available
  - AS's generate Route Origination Authorizations (ROA's)
    - Associates address prefix, with AS number giving the AS permission to advertise the prefix
    - ROA is signed with requesting AS private key
  - Some RIR's provide RPKI, such as RIPE NCC
    - Validates routing information, variety of tools and resources on subject
- **Caveats**
  - Can be defeated. Add authorized AS number to end of AS_PATH.
  - Announcement messages are not signed
  - RPKI only validates that the AS path is correct, more secure solutions such as BGPSec should be used

Countermeasure … 3

- **BGPSec**
  - Based on path attribute BGPSEC_Path, replaces AS_PATH.
  - Carries AS Path information, along with digital signatures in sequence to update message
    - Alterations to AS Path or NLRI detected by receiving AS
  - BGPSec aware routers advertise support in open messages
  - Uses centralized government-like body (E.g IANA) PKI Infrastructure
- **Caveats**
  - Higher memory footprint – Multiple signatures, more memory use
  - Router must possess the capability to validate cryptographic signatures received
  - Side effect – Seize range of IP addresses, spoof them, or even a single address. US Government? Censorship?

Countermeasure … 4

- **MD5 Neighbour Authentication**
  - Each segment sent over TCP connection between peers is verified
  - Provides authentication, whereas BGP usually lacks this
  - Not enabled by default

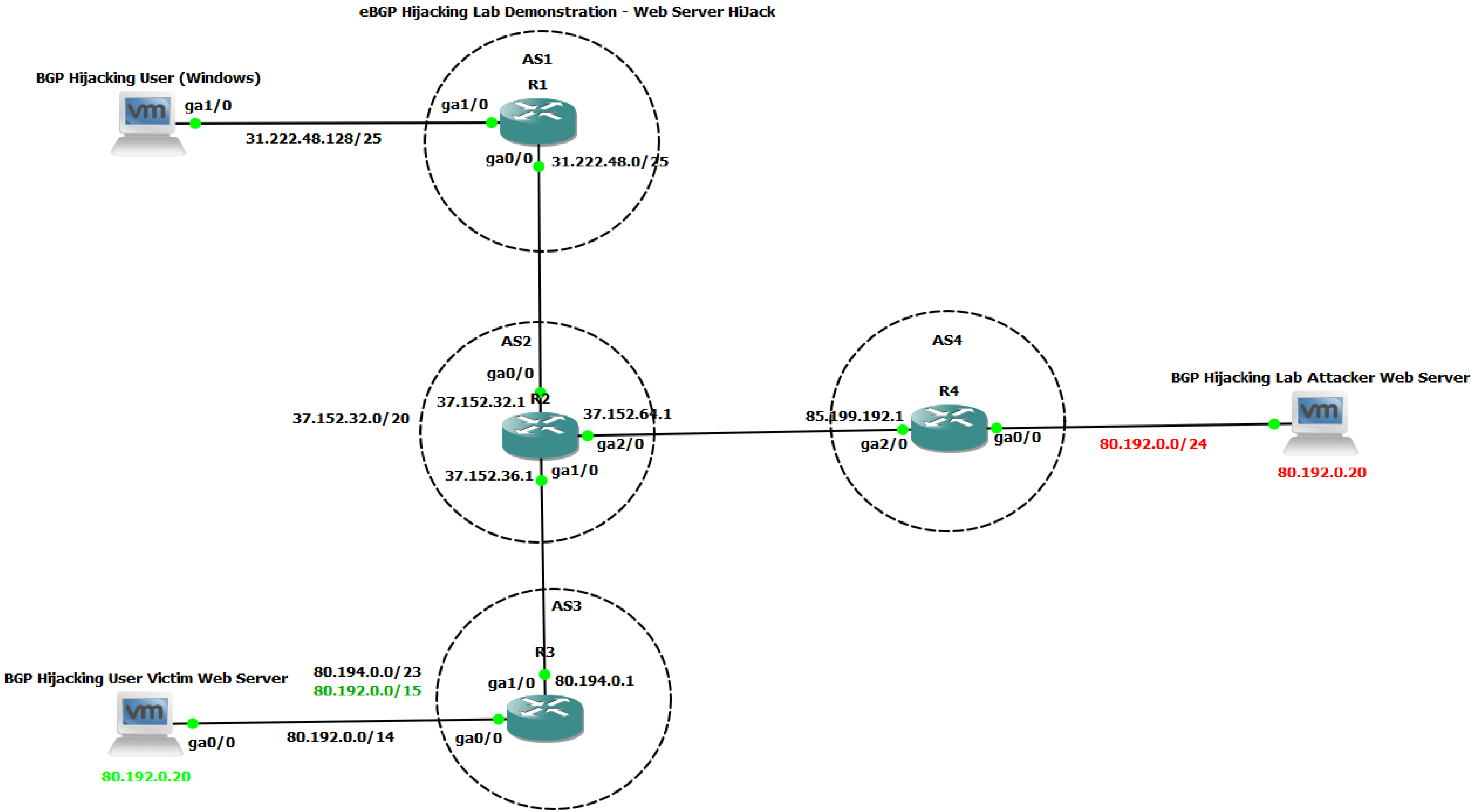
  - **Caveats**
    - MD5 can be broken easily, MD5 digest being phased out
      - Brute force attacks

Countermeasure … 5

- **Best Practices**
  - Best practices should be followed as per manufacture
    - E.g Cisco provides lots of documentation on BGP configuration
  - Defence in depth, protects against more attacks than BGP hijacking
    - TCP Reset attacks, spoofing ect
- **Caveats**
  - None! No excuse for not following **SOME** or **ALL** best practices

Demo

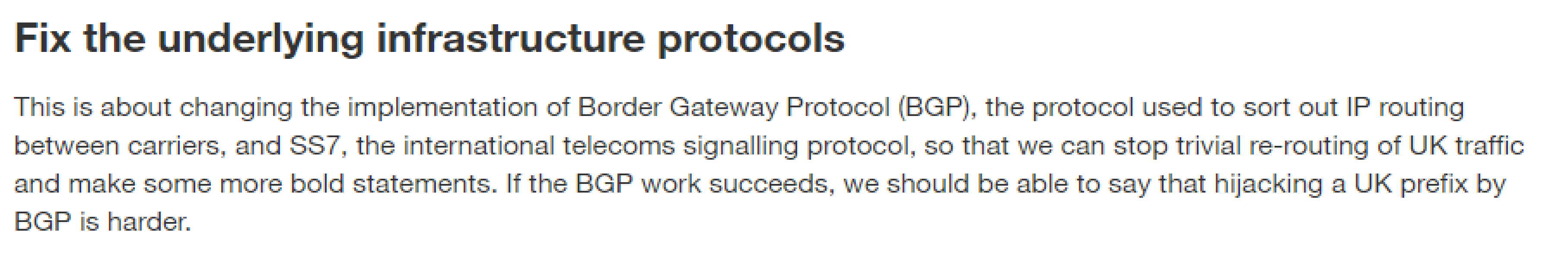
- GNS3 + VMWare Workstation Pro
  - TurnKey Linux Web Servers (NGINX PHP-FPM)
  - Windows 10 Client
  - 4 Autonomous Systems + C7200 Cisco Routers
  - /15 Prefix


eBGP Hijacking Lab Demonstration - Web Server HiJack
AS1
R1
BGP Hijacking User (Windows)
ga1/0
ga1/0
31.222.48.128/25
ga0/0
31.222.48.0/25
AS2
ga0/0
37.152.32.1
R2
37.152.32.0/20
37.152.64.1
ga2/0
37.152.36.1
ga1/0
AS4
R4
85.199.192.1
ga2/0
ga0/0
BGP Hijacking Lab Attacker Web Server
80.192.0.0/24
80.192.0.20
AS3
R3
80.194.0.0/23
80.192.0.0/15
ga1/0
80.194.0.1
BGP Hijacking User Victim Web Server
ga0/0
80.192.0.0/14
ga0/0
80.192.0.20

NCSC & Government Strategy

- **National Cyber Security Centre** (NCSC) was announced in 2015
  - Part of National Cyber Security Plan
  - "Active" Cyber Defence plan to be implemented, announced 1st November 2016
  - Plans to defeat BGP prefix hijacking in the UK, or make it more difficult.

National Cyber Security Centre
a part of GCHQ



Fix the underlying infrastructure protocols

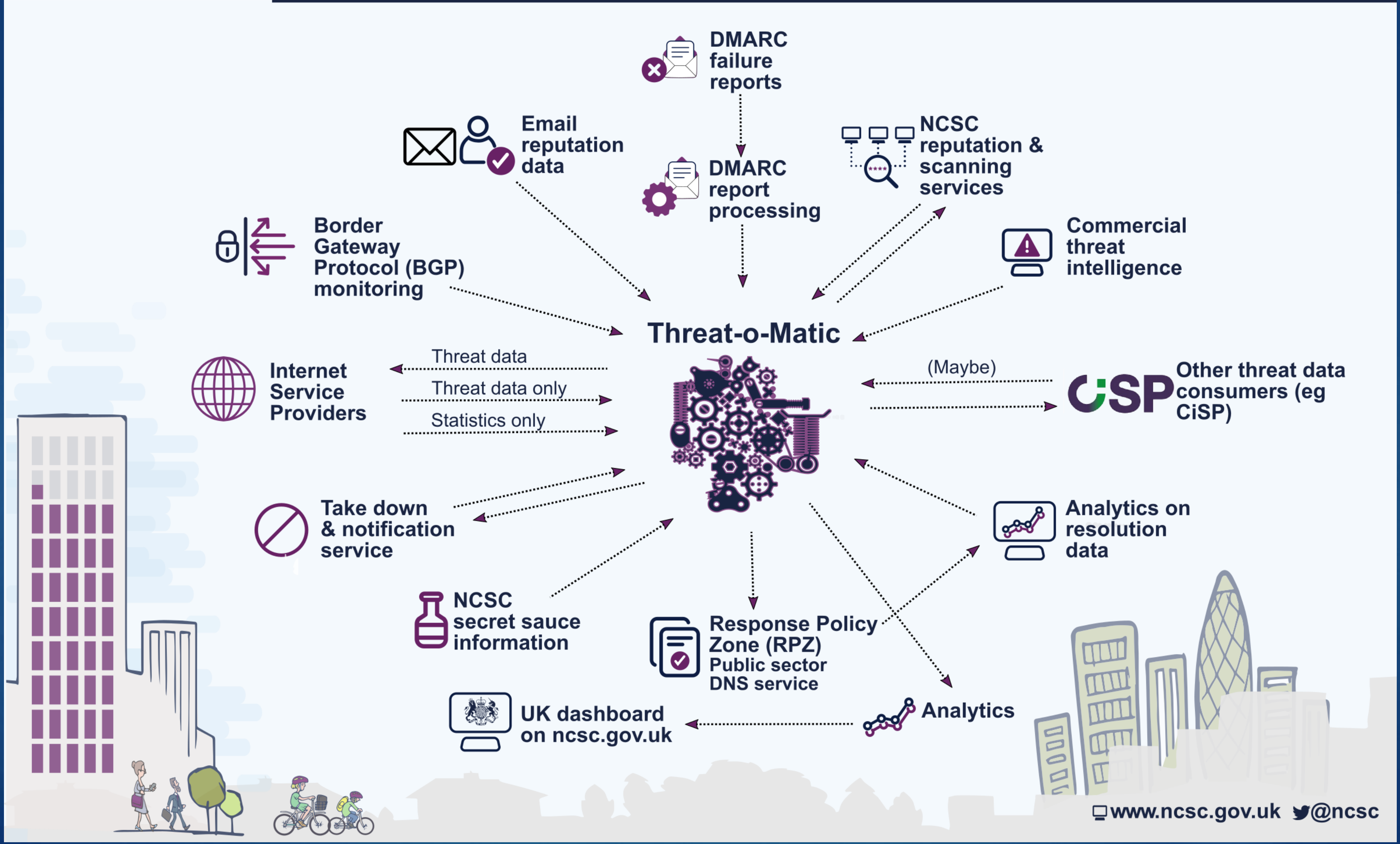
This is about changing the implementation of Border Gateway Protocol (BGP), the protocol used to sort out IP routing between carriers, and SS7, the international telecoms signalling protocol, so that we can stop trivial re-routing of UK traffic and make some more bold statements. If the BGP work succeeds, we should be able to say that hijacking a UK prefix by BGP is harder.

https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk

National Cyber Security Centre

Active Cyber Defence

The Active Cyber Defence (ACD) Programme outlines how the NCSC intends to tackle - in a relatively automated way - many of the cyber attacks that hit the UK. The diagram below is **not** an architecture, so not all these initiatives will be in place at day one.



Threat-o-Matic

DMARC failure reports

DMARC report processing

Email reputation data

NCSC reputation & scanning services

Border Gateway Protocol (BGP) monitoring

Commercial threat intelligence

Internet Service Providers

Threat data

Threat data only

Statistics only

(Maybe)

Other threat data consumers (eg CiSP)

Take down & notification service

Analytics on resolution data

NCSC secret sauce information

Response Policy Zone (RPZ) Public sector DNS service

Analytics

UK dashboard on ncsc.gov.uk

www.ncsc.gov.uk @ncsc

Was BGP Ever Great

Maybe in 1990

Trust by default routing, does not work in the modern world

Thank you.

Questions

Twitter: @MrJamesHemmings

Email: james@hemmings.pw

LinkedIn: https://uk.linkedin.com/in/jhemmings

Blog: https://blog.jameshemmings.co.uk

Web: https://jameshemmings.co.uk