Are We Ready for a Traffic Redirection?

Eugene Bogomazov
Qrator Labs

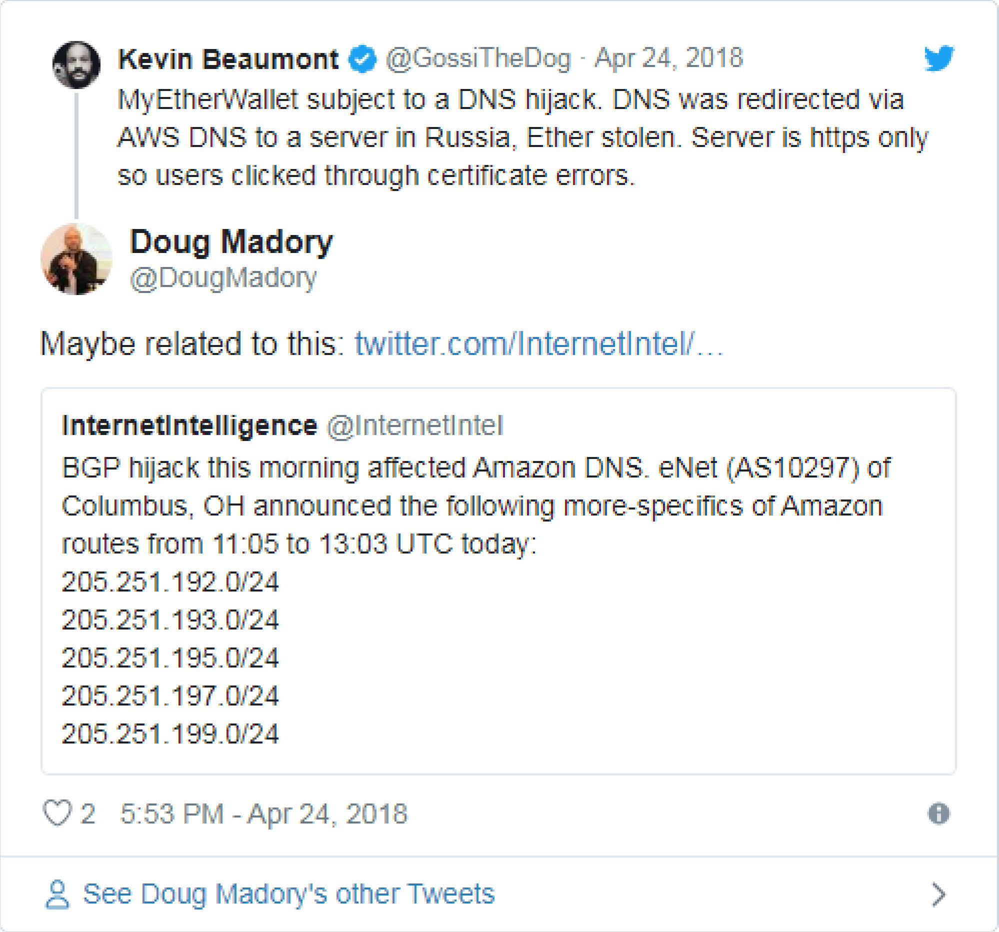
What it's not about

- ***That*** kind of redirection
  - Goverment control
  - Centralised routing

What it's all about

- Normal BGP hijacks
  - With malformed AS_PATH
  - And valueable profit
- Future of monitoring
  - And headache for RIPE routing police
- Future of BGP security

Reminder



Kevin Beaumont @GossiTheDog · Apr 24, 2018

MyEtherWallet subject to a DNS hijack. DNS was redirected via AWS DNS to a server in Russia, Ether stolen. Server is https only so users clicked through certificate errors.

Doug Madory
@DougMadory

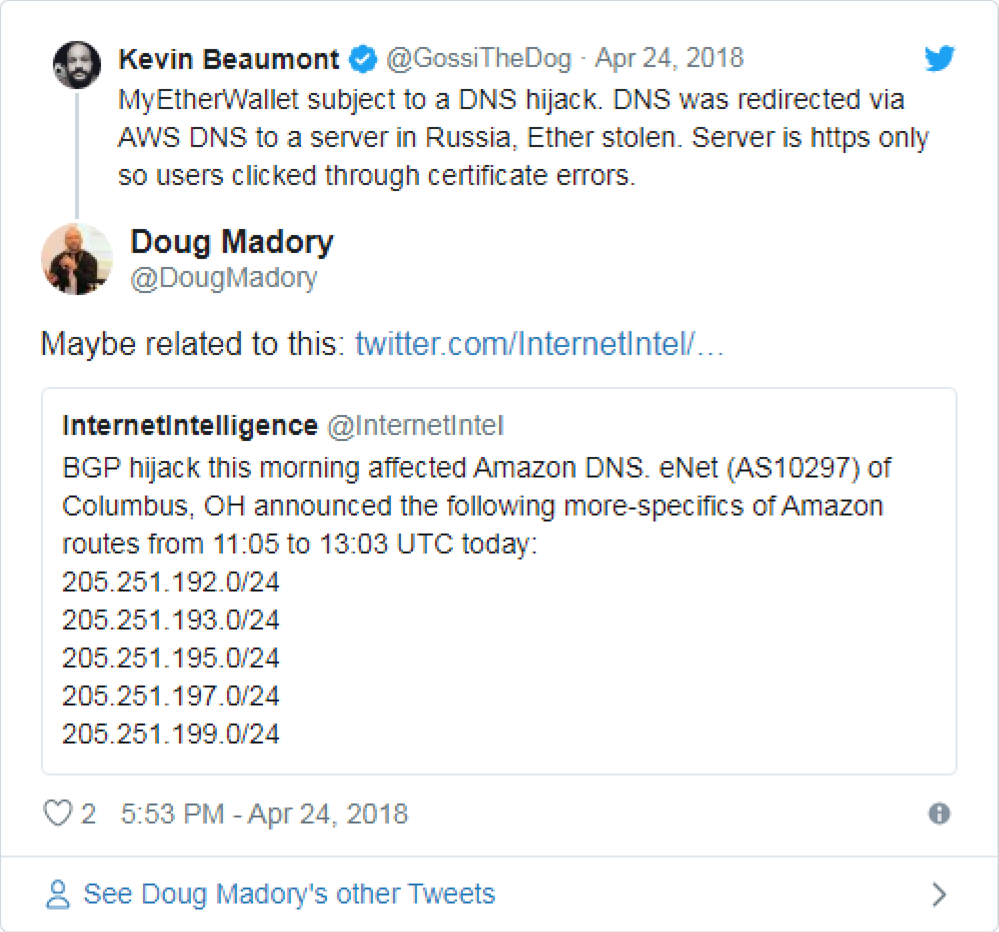
Maybe related to this: twitter.com/InternetIntel/…

InternetIntelligence @InternetIntel

BGP hijack this morning affected Amazon DNS. eNet (AS10297) of Columbus, OH announced the following more-specifics of Amazon routes from 11:05 to 13:03 UTC today:
205.251.192.0/24
205.251.193.0/24
205.251.195.0/24
205.251.197.0/24
205.251.199.0/24

♡ 2 5:53 PM - Apr 24, 2018

News PoV



Kevin Beaumont @GossiTheDog · Apr 24, 2018

MyEtherWallet subject to a DNS hijack. DNS was redirected via AWS DNS to a server in Russia, Ether stolen. Server is https only so users clicked through certificate errors.

Doug Madory
@DougMadory

Maybe related to this: twitter.com/InternetIntel/…

InternetIntelligence @InternetIntel
BGP hijack this morning affected Amazon DNS. eNet (AS10297) of Columbus, OH announced the following more-specifics of Amazon routes from 11:05 to 13:03 UTC today:
205.251.192.0/24
205.251.193.0/24
205.251.195.0/24
205.251.197.0/24
205.251.199.0/24

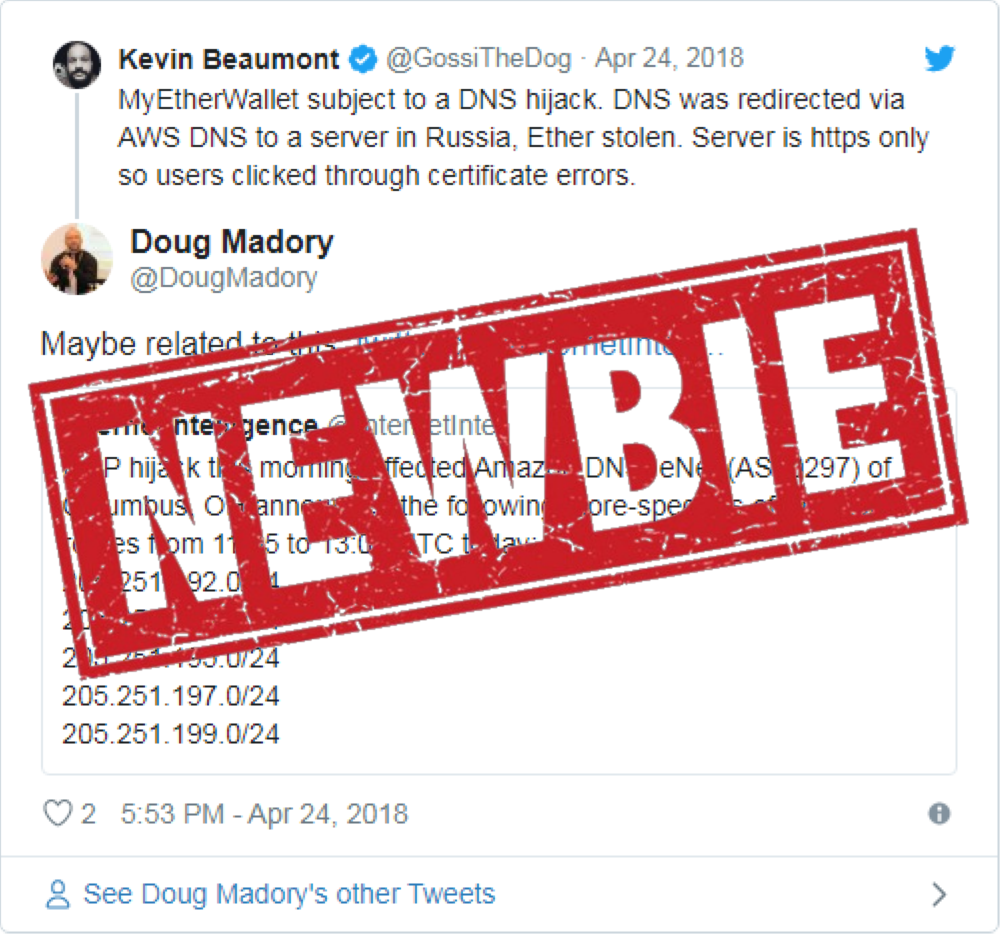
♡ 2 5:53 PM - Apr 24, 2018

See Doug Madory's other Tweets

- BGP Hijack
- Of public DNS
- More than 100k$ loss

- Cool guys
- Routing as an attack vector

~~Normal~~ Our PoV



Kevin Beaumont @GossiTheDog · Apr 24, 2018

MyEtherWallet subject to a DNS hijack. DNS was redirected via AWS DNS to a server in Russia, Ether stolen. Server is https only so users clicked through certificate errors.

Doug Madory
@DougMadory

Maybe related to th[illegible] ...ernetInt...

[illegible]nte[illegible]gence @[illegible]ter[illegible]etInte[illegible]

[illegible]P hija[illegible]k t[illegible] mo[illegible]ning [illegible]ffected Amaz[illegible] DN[illegible] eNe[illegible] (AS[illegible]297) of C[illegible]umbus, O[illegible] anno[illegible] the fo[illegible]owin[illegible] more-spe[illegible] [illegible]es f[illegible]om 11[illegible]5 to 13:0[illegible] UTC t[illegible]day:
[illegible]251.[illegible]92.0/[illegible]4
2[illegible]
2[illegible]
2[illegible].195.0/24
205.251.197.0/24
205.251.199.0/24

2 5:53 PM - Apr 24, 2018

See Doug Madory's other Tweets

NEWBIE

- Old type of attack
- Origin ASN in AS_PATH?!
- Self-signed certificates??!

- Can the attack be more:
  - Successful?
  - Stealth?

Can the attack be…?

Yeap

BGP 101

- Internet is a network of ASes
- BGP — only protocol of communication
- Exchange information via routes
- Routes contain information about prefix
    - And nexthop
- Most interesting attribute — AS_PATH

- O RLY? N in E**N**OG is for Network...

Threat model

- Too many enemies around
  - Even ourselves
- So let“s make a double check
  - Who if not us?
- Anything can be changed
  - Especially prefix and AS_PATH

Redirection motivation

- Human error
  - *Monkey***iTM**
- Traffic blackholing/listening
  - *Man***iTM**
- Get the remaining part of traffic
  - Money, money, money
  - Unhealthy competition

BGP Hijacks

- Announce of foreign address space
  - Whom to trust?

**Game: Find Spartacus*

Routing 101?

- Which direction to send packet?
- Forwarding:
  - Longest prefix match
- Routing:
  - Local pref (Customer > Peer > Provider)
  - AS_PATH length

- No more ***101***
  - Promise

Five shades of Hijacks

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- AS_PATH manipulation *(sub-prefix + valid AS_PATH)*

Last but not least

- Take a valid route
- Retrieve prefix and AS_PATH
- Split prefix onto two halves
- Announce these prefix with AS_PATH
- ???
- Get almost all the traffic to yourself

How it works

- Loop detection
  - Doesn“t seen by AS from valid AS_PATH
- Longest prefix match
  - Lures the traffic
- ??? - static route
  - Returns traffic onto backup path

Connectivity battle

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- AS_PATH manipulation

** In regions where both routes are seen*

Guided stone

- Prevention
  - Mark your own information
  - To help others filter bad guys
- Monitoring
  - Find cases of abuse
  - And find out who made them
- Mitigation
  - Return traffic to the base

Step one

- **Prevention**
  - **Mark your own information**
  - **To help others filter bad guys**
- Monitoring
  - Find cases of abuse
  - And find out who made them
- Mitigation
  - Return traffic to the base

Another POV

- IRR
  - AS_SET + route objects
  - Usually prefix whitelist of Customer Cone
  - Needed for global connectivity
- ROA/RPKI
  - Prefix + origin ASN check
  - Needed to prevent others
  - Which maxLength to use?

Problem with length

- IRR
  - Exact/covered type of choice
  - Make independently, but more often the second
  - No uniform standard
- ROA/RPKI
  - **Valid cases** vs **hijacks**
  - Not implemented everywhere
  - Not «drop Invalid» everywhere where implemented

Prefix + origin check

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- AS_PATH manipulation

Prefix + CC check

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- AS_PATH manipulation

** You will not see a hijack made between CC members*

*** The quality of filter can be very poor*

Exact match/equal maxLength

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- AS_PATH manipulation

AS_PATH manipulation

- Make AS_PATH shorter
- Add ASNs to avoid these ISPs
- Use AS_PATH from other route

Manipulation examples

- Route Leak prevention
- Link load balancing
- Link overloading
- Pilosov-Kapela
    - More correct name for fifth hijack type
    - Real example (Beginning of our story)

Basic AS_PATH filters?

- Bogon ASN
- TIER_1 filtering
- Neighbor check
  - Exception: IXP RS
  - Your ASN must be in AS_PATH

- Seems to not help...

AS_PATH verification

	BGPSec	ASPA
Main goal	Stop crafted routes	Stop global propagation
AS_PATH + NLRI	Yes	Only AS_PATH
AS_PATH validation	Is real?	Is valid?
Cryptographic load	For each route in each direction	Only during filter creation
Partial deployment	For «connected islands»	For independent deployment
Prevent route leaks	With draft extension	As a side effect
Status	RFC; not spreaded	Draft; waiting

BGPSec

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- Pilosov-Kapela

**But replay attack is still remaining...*

ASPA

- Tradional ones:
  - ”Global Hijacking” -> sub-prefix
  - “Local Hijacking” -> equally-specific-prefix
- Prepended ones:
  - sub-prefix
  - equally-specific-prefix
- Pilosov-Kapela
  - AS_PATH is valid
  - Propagation in all directions
  - Is sub-prefix covered with maxLength?

Prefix filtering vs ASPA

- Common:
  - Same scope of hijacks
  - Cannot be use on p2c link
  - Goal: stop the global propagation
- For prefix filter the hijack within CC is invisible
- Different world views
  - «Pass the check» vs «Stop the others»

Investigation step

- Prevention
  - Mark your own information
  - To help others filter bad guys
- **Monitoring**
  - **Find cases of abuse**
  - **And find out who made them**
- Mitigation
  - Return traffic to the base

Monitoring sub-prefix

- Ground truth about prefixes
  - In a dynamic way
- Information about routes
  - BGP collector
- Combine previous points
  - ARTEMIS

- In out case: BGP sessions + our collector + analytics

Monitoring manipulation

- BGP collector
  - Many different routes
- Neighbor check
  - ASN in AS_PATH
- Become a critical point
  - All roads are lead through the attacker

Monitoring challenges

- False positive:
  - One legs
  - Normal critical points
- False negative:
  - Absence of neighbor check
  - Attack from two or more AS
    - Hard to organize a backup route
    - Still abnormal route graph

Unavoidable step

- Prevention
  - Mark your own information
  - To help others filter bad guys
- Monitoring
  - Find cases of abuse
  - And find out who made them
- **Mitigation**
  - **Return traffic to the base**

Mitigation

- Write a letter!
- Announce the valid most specific prefix
  - If longer — win, if equal — battle
- Create new registration object?
  - Too long to wait (several hours to apply)
  - Not help with /24(/48) attack due to too specific
  - Can make even worse in corner cases

HiSHE

- **Be ready** to announce the most specif one
  - So, you“ll have the equal prefix length
- How to win the connectivity battle?
  - Increase your own (Tier-1 connections, IXes, etc)
  - Or delegate
  - Attacker might have +1 to length anyway
    - To avoid ROA validation

Are you ready?

- If you are monitoring your prefixes — yes
  - Pilosov-Kapela will be gone
- Unfortunately, the battle is yet unavoidable
  - Unless the ASPA will be adopted in the wild

- Mitigation doesn“t require to know the attacker ASN
  - Because sometimes it can be really hard

Questions?

Contacts: eb@qrator.net