Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks

Network and Distributed System Security (NDSS) Symposium
San Diego, February 2015

Pierre-Antoine Vervier[†§], Olivier Thonnard[†], Marc Dacier[‡]

Symantec Research Labs[†], Eurecom[§], Qatar Computing Research Institute[‡]

Where it all started

> **(BGP Spectrum Agility)** *[…] spammers appear to send spam by (1) advertising (in fact, hijacking) large blocks of IP address space (i.e., /8s), (2) sending spam from IP addresses […], and (3) withdrawing the route for the IP address space shortly after the spam is sent.*

A. Ramachandran and N. Feamster. *Understanding the Network-level Behavior of Spammers*, ACM SIGCOMM, 2006

Security issues

- Impact **IP-based reputation** systems, such as spam blacklists used as a first layer of defence in spam filters
- **Misattribute** attacks launched from hijacked networks due to hijackers stealing **IP identity**

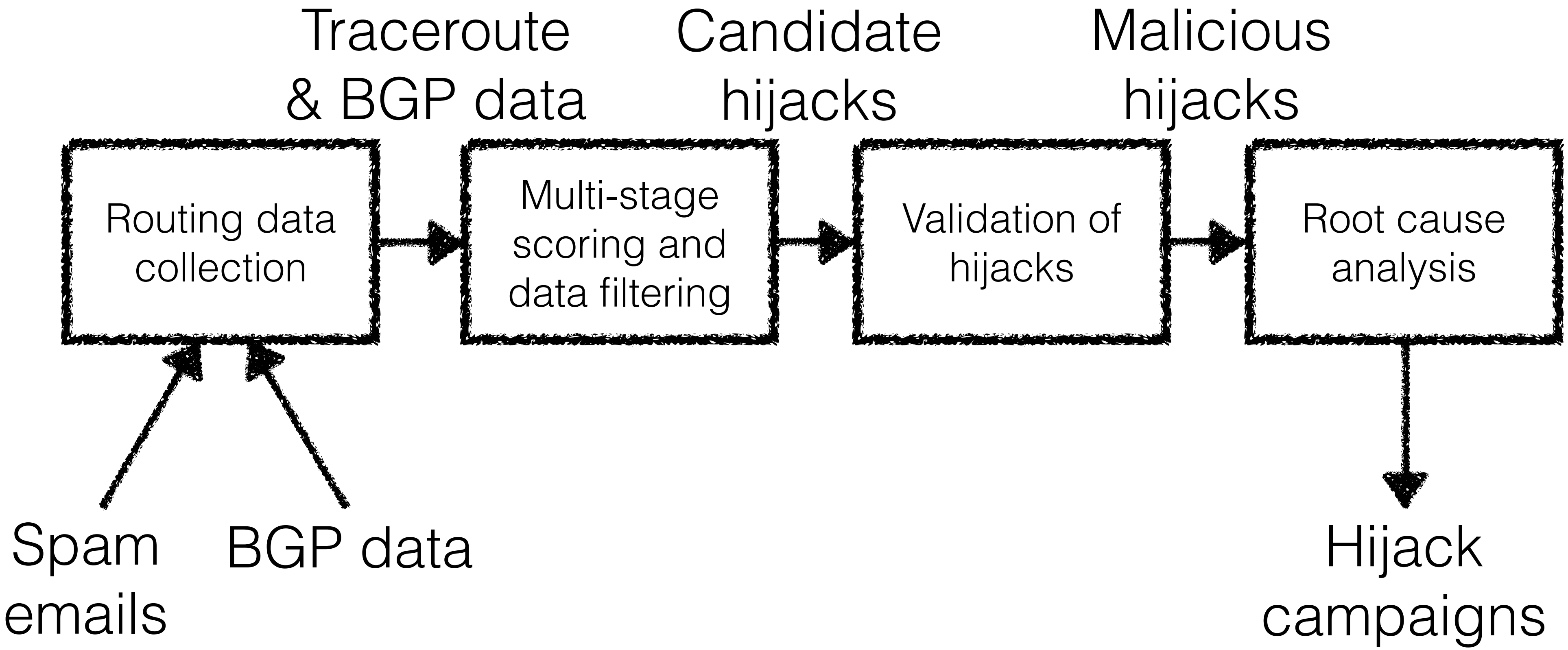
Border Gateway Protocol (BGP)

- The Internet is divided into thousands of smaller networks called **Autonomous Systems (ASes)**
    - e.g., an Internet Service Provider (ISP), a company, a university
- **Routing** between ASes is achieved using the Border Gateway Protocol (BGP) to
    - Advertise to others the IP addresses of their network
    - Receive the routes to reach the other ASes

BGP hijacking

- Injection of **erroneous** reachability information into BGP
  - **Trust**-based exchange of reachability information between ASes
  - **No** widely deployed security mechanism yet

Experimental environment



Traceroute & BGP data

Candidate hijacks

Malicious hijacks

Routing data collection

Multi-stage scoring and data filtering

Validation of hijacks

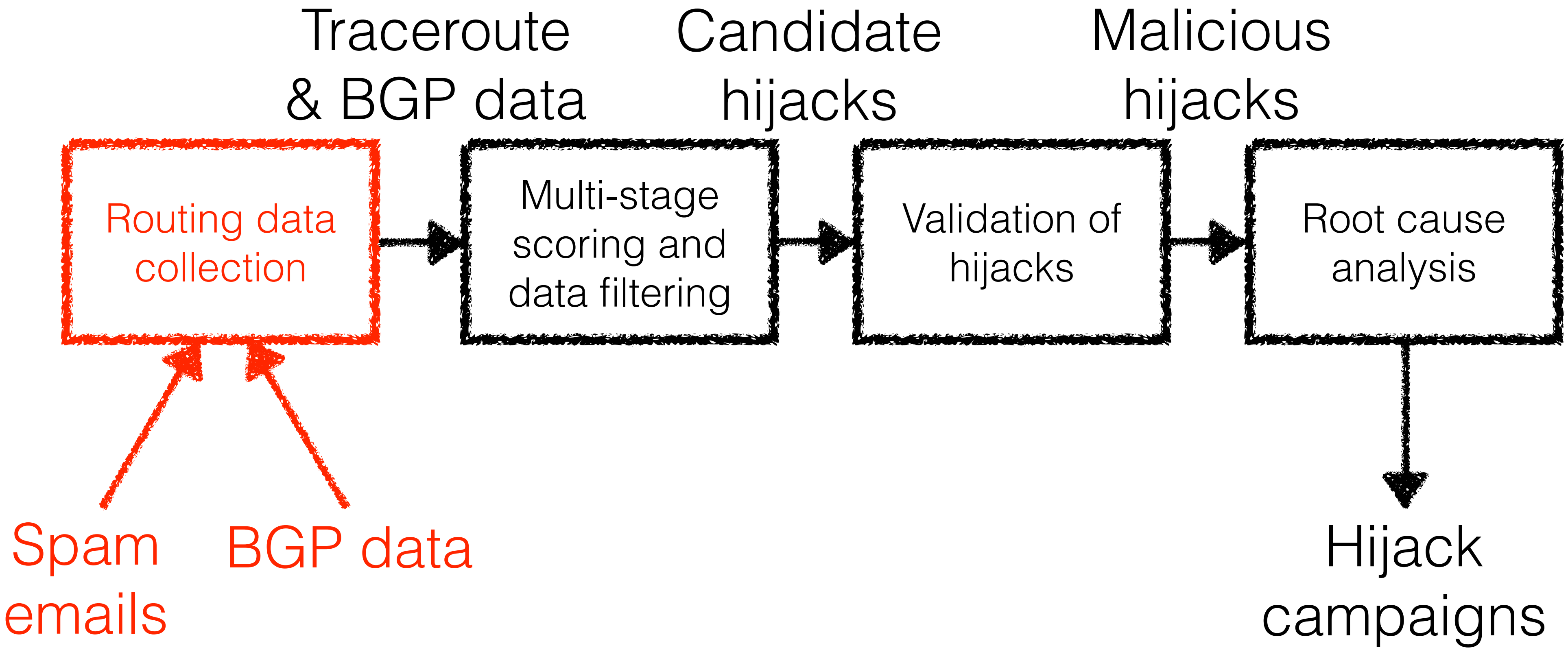
Root cause analysis

Spam emails

BGP data

Hijack campaigns

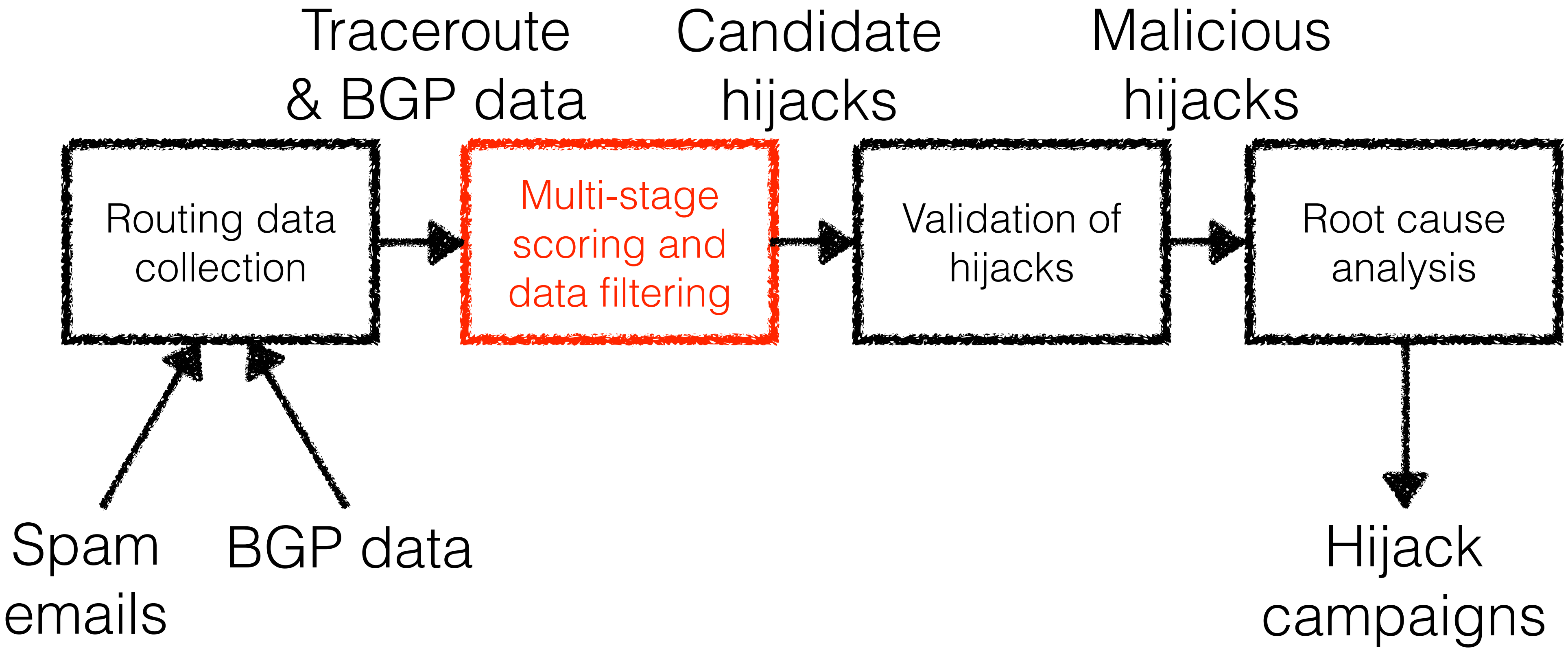
Results


Traceroute & BGP data
Candidate hijacks
Malicious hijacks
Routing data collection
Multi-stage scoring and data filtering
Validation of hijacks
Root cause analysis
Spam emails
BGP data
Hijack campaigns

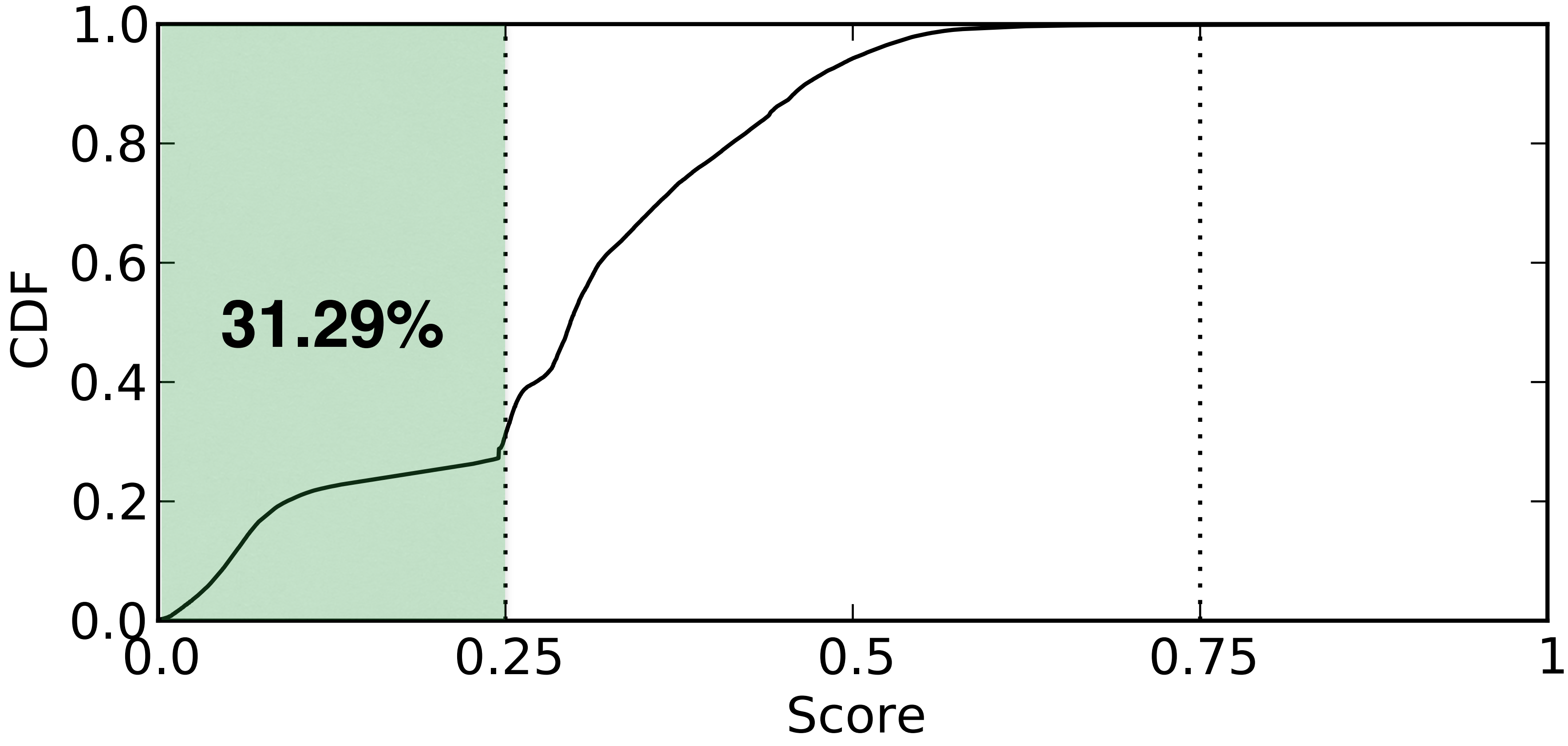
Routing data collection

- Between Jan’13 and Jun’14 (18 months)
  - 391,444 distinct IP address blocks monitored
  - 18,252 distinct ASes (~40% of active ASes)
  - 5,594,164 traceroutes
  - 25,679,725 BGP routes

Results

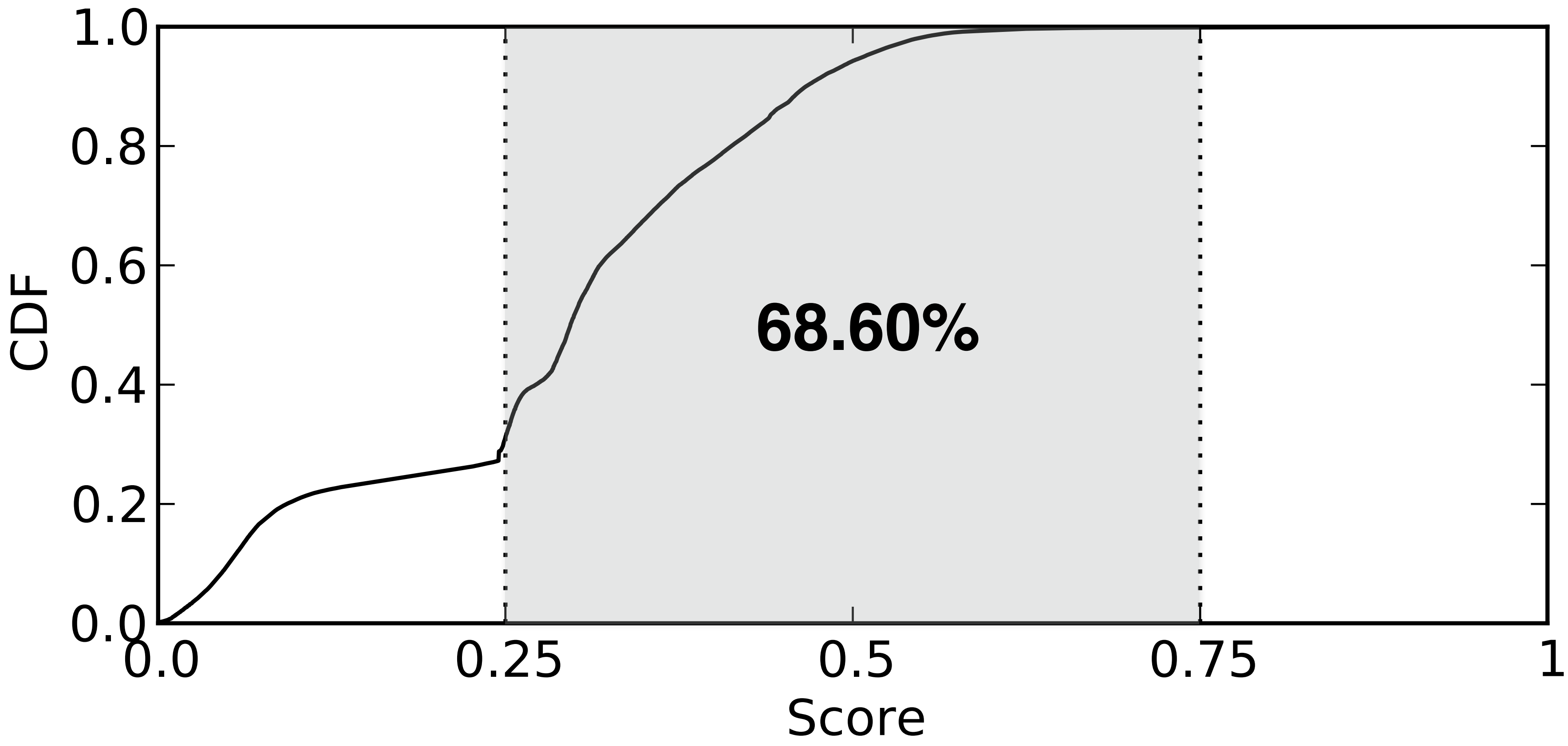

Traceroute & BGP data
Candidate hijacks
Malicious hijacks
Routing data collection
Multi-stage scoring and data filtering
Validation of hijacks
Root cause analysis
Spam emails
BGP data
Hijack campaigns

Candidate hijacks



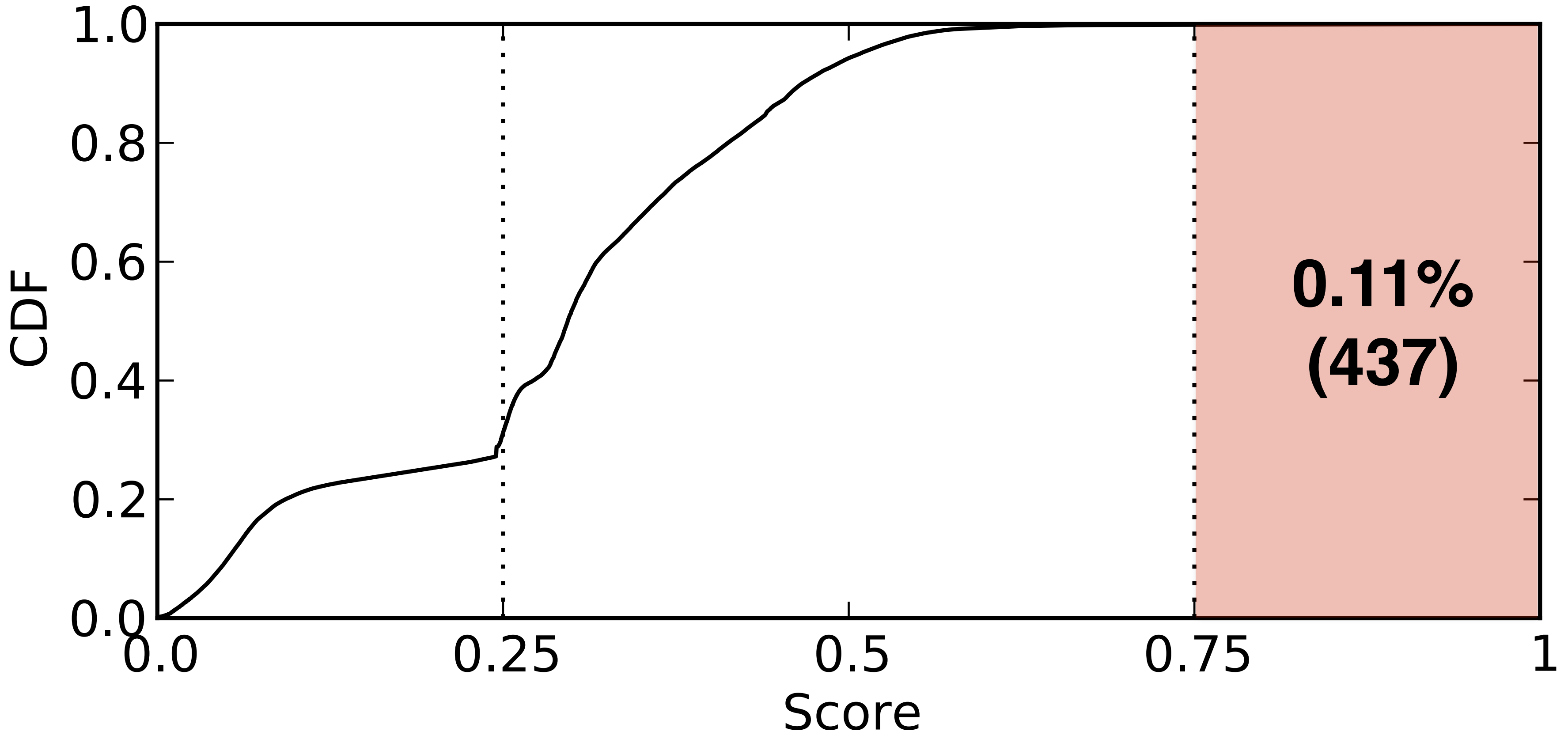
Very likely benign!

Candidate hijacks



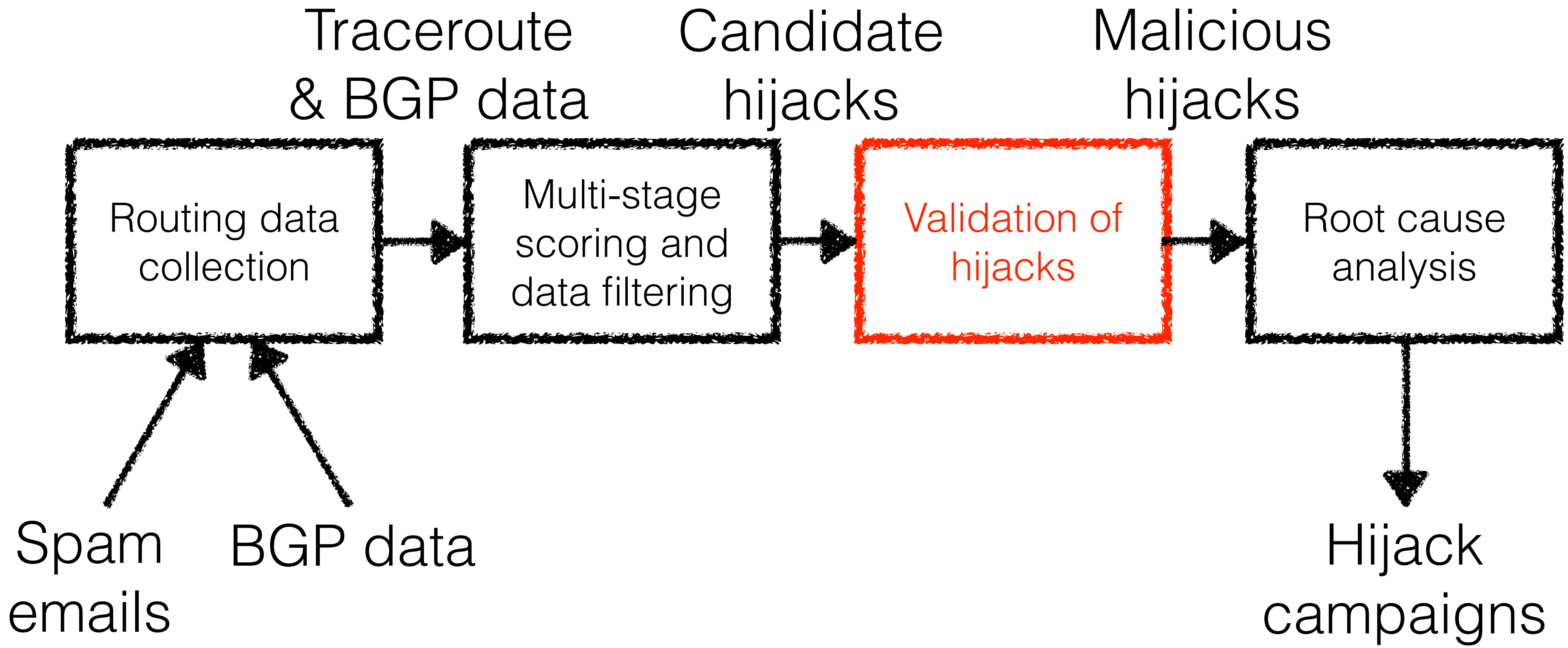
Grey zone: hard to attribute to benign or malicious behavior!

Candidate hijacks



Most likely hijacked networks!

Results


Traceroute & BGP data
Candidate hijacks
Malicious hijacks
Routing data collection
Multi-stage scoring and data filtering
Validation of hijacks
Root cause analysis
Spam emails
BGP data
Hijack campaigns

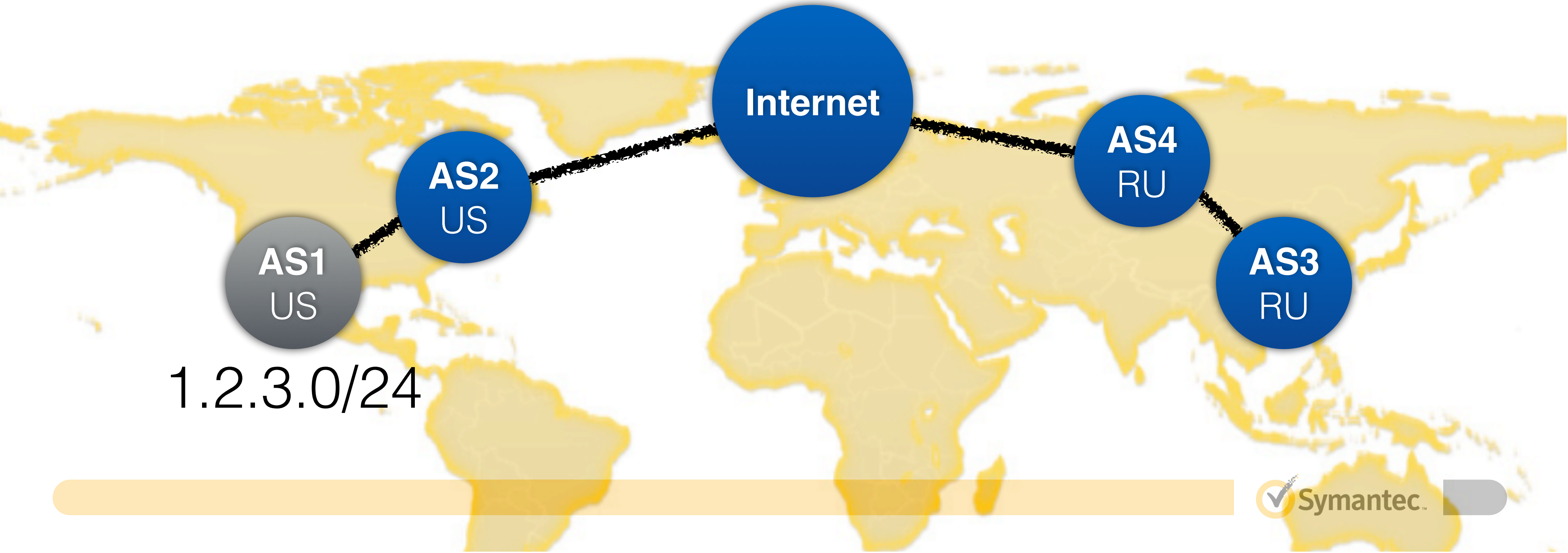
Malicious BGP hijacks

- **64** (out of 437) validated malicious BGP hijacks
- Hijacked IP address blocks were **dormant**, i.e., they had been left idle by their owner
- **Two** hijack categories:
  - Prefix hijack via valid upstream
  - AS hijack via rogue upstream

1. Prefix hijack via valid upstream

92% of hijacks

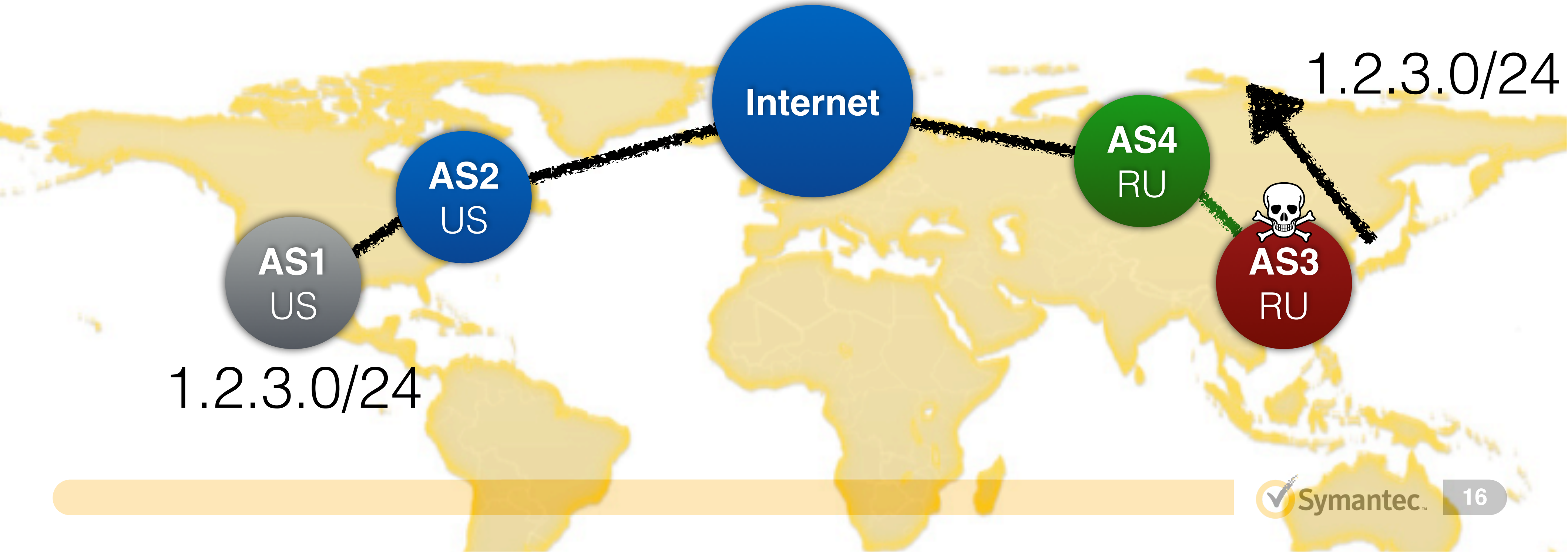
- Advertised by an **invalid** BGP origin AS…
- …but via **valid** direct upstream provider (first hop) AS



1. Prefix hijack via valid upstream

92% of hijacks

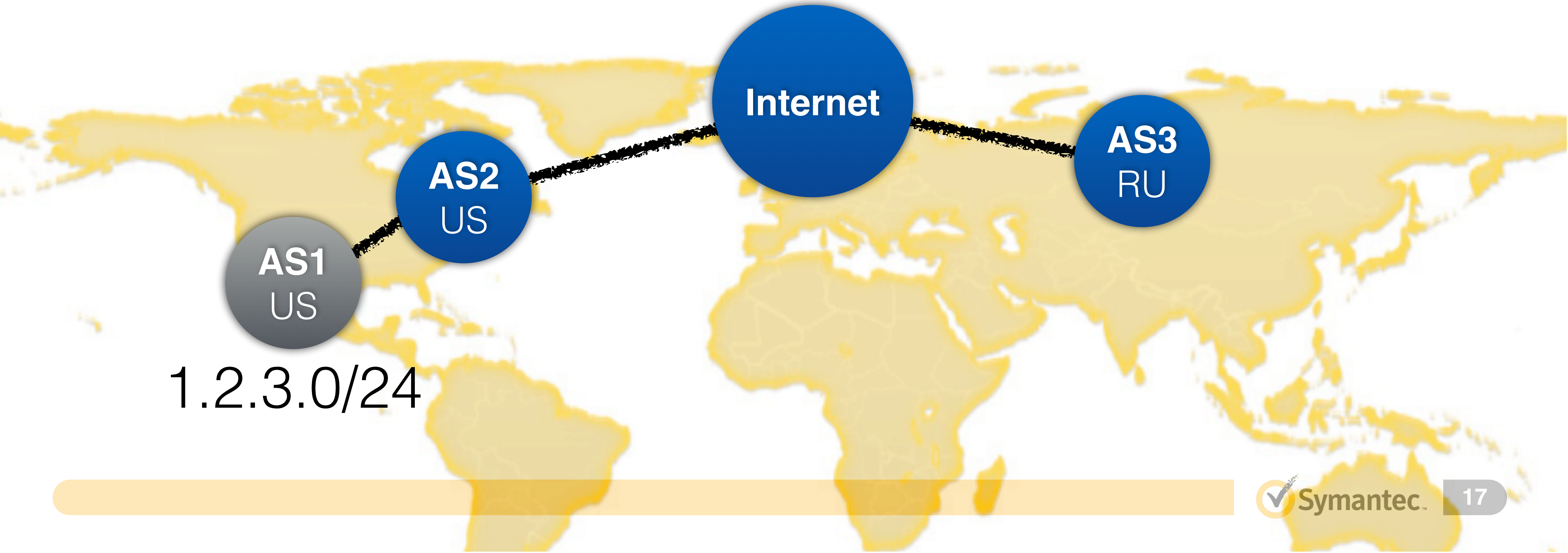
- Advertised by an **invalid** BGP origin AS…
- …but via **valid** direct upstream provider (first hop) AS



2. AS hijack via rogue upstream

8% of hijacks

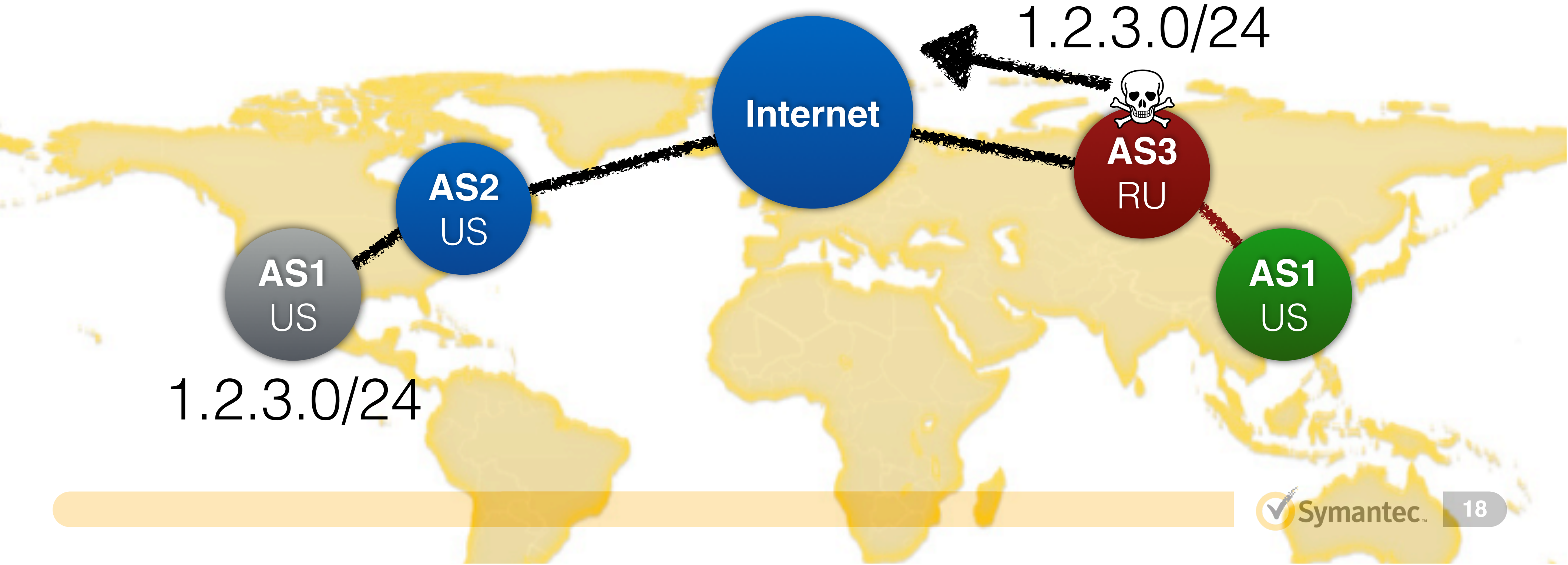
- Advertised by a **valid** BGP origin AS…
- …but via a **rogue** direct upstream provider (first hop) AS



2. AS hijack via rogue upstream

8% of hijacks

- Advertised by a **valid** BGP origin AS…
- …but via a **rogue** direct upstream provider (first hop) AS



Let’s pull on the rope…

- 64 validated hijacked IP address blocks
  - … were advertised by/via 10 invalid ASes
  - … have sent spam to our spamtraps
- Between Jan’13 and Jun’14, 2,591 other IP address blocks
  - …were advertised by/via these 10 invalid ASes
  - …have not sent spam to our spamtraps

…and do the math

64 + 2591

=

2,655 IP address ranges hijacked between Jan’13 and Jun’14

Tell me more, tell me more…

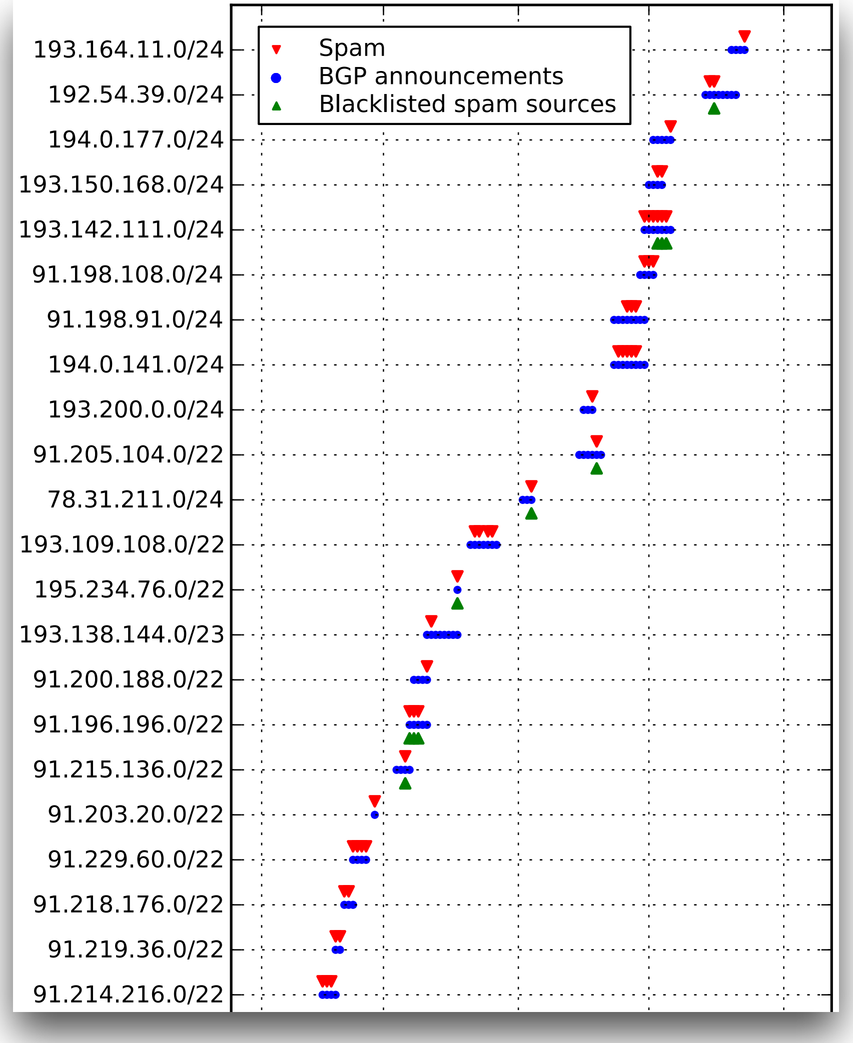
- How long do hijacks last?
- How effective is this spamming technique?
- What about those not used for sending spam?

Two hijack phenomena

- **Short-lived** (98.7%)
  - Last from a few minutes to 1 week
  - 85.5% last less than 1 day (similar to Ramachandran et al., SIGCOMM'06)
- **Long-lived** (1.3%)
  - Last from 1 week to several months

How effective is this spamming technique?

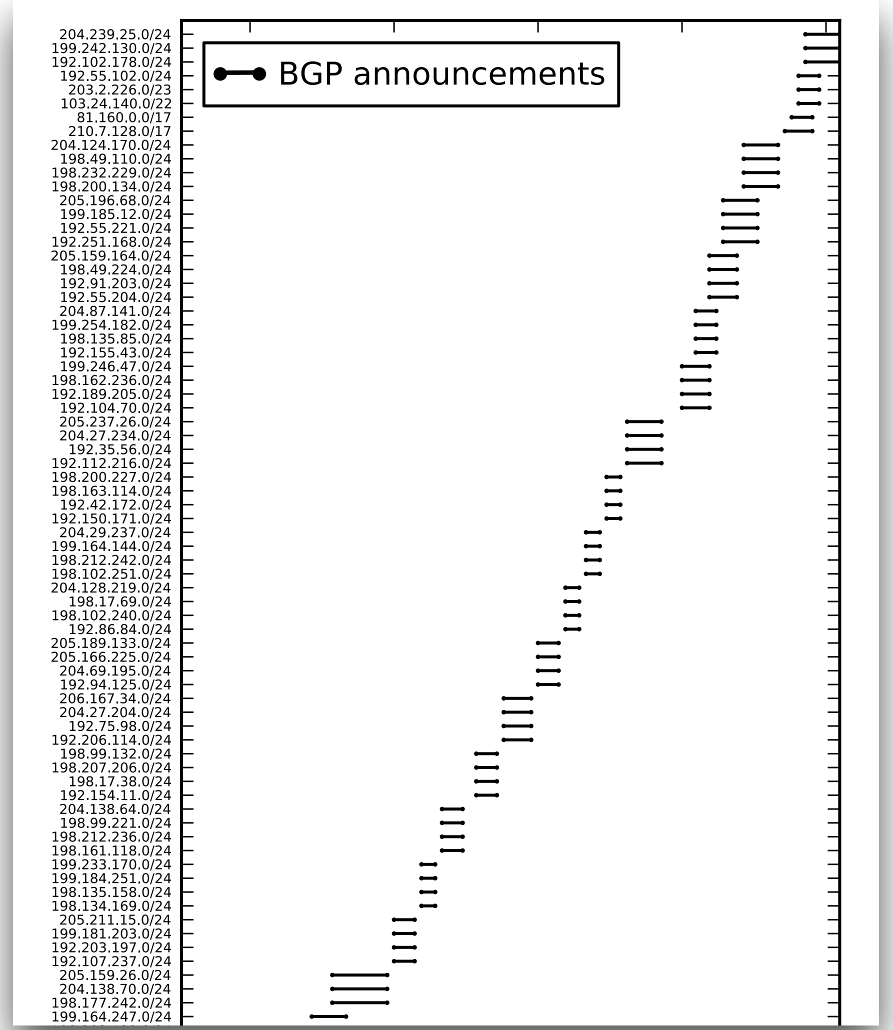
- Out of the 2,655 hijacked address blocks
  - 64 sent spam to our spamtraps
  - 13 were blacklisted in Spamhaus SBL & DROP, Uceprotect and Manitu
- **Spamming from hijacked networks appears to be effective against spam IP blacklists!**



Symantec.

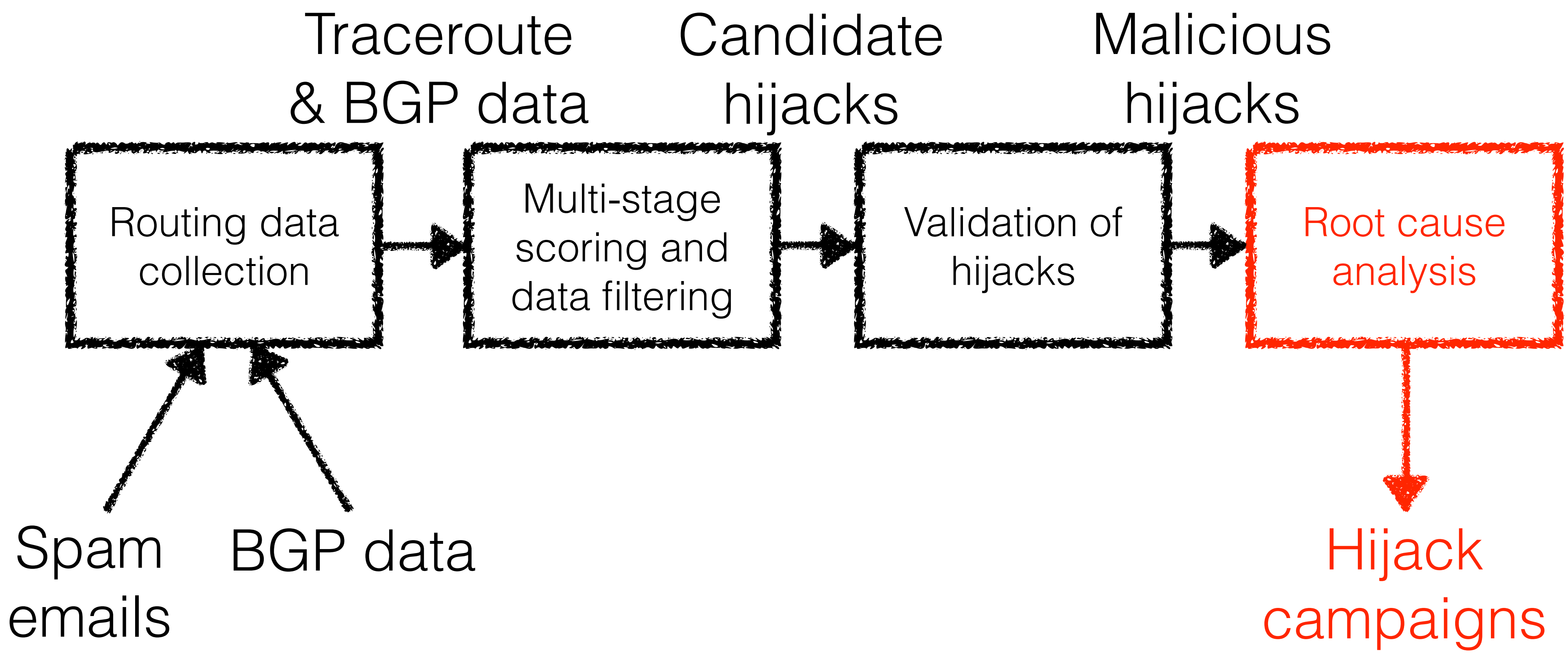
Automated hijack machine?

- Between Jun'13 and Jun'14
  - 2,562 short-lived hijacked IP blocks
  - always performed by groups of 2 to 4 prefixes
  - hijacks in group start and end at the same time
  - always at least two prefixes hijacked during 13 months
  - no spam!



Full picture available at http://bit.ly/ndss2015_bgphijacks_episode2

Results



Traceroute & BGP data

Candidate hijacks

Malicious hijacks

Routing data collection

Multi-stage scoring and data filtering

Validation of hijacks

Root cause analysis

Spam emails

BGP data

Hijack campaigns

Hijack campaigns

- ~5K spam emails received from 64 hijacked prefixes
- Three types of spam campaigns identified by TRIAGE
  - 10x single prefix not abused elsewhere
  - 17x single prefix abused in other campaigns
  - **3x multiple prefixes abused sequentially over a long period of time→agile spammers!**

Lessons learned and conclusions

- As of today “BGP spectrum agility” is still a problem worth of consideration
  - persistent and stealthy campaigns of malicious BGP hijack
- Today’s BGP hijack mitigation systems are easily defeated by sophisticated hijack attacks
- As of today, about 20% of the IPv4 address is allocated but not publicly announced➔vulnerable to hijacking!

Lessons learned and conclusions (cont.)

- Uncovered hijacks involved many IP address blocks but few invalid ASes➔proactive detection!
- As future work, expand the collaboration with CERTs, ISPs and the NANOG & RIPE communities to help mitigate malicious BGP hijacks
  - E.g., discussions with CERT.be and an unwittingly involved ISP confirmed 793 hijacks

Thank you!
Questions?

Pierre-Antoine Vervier
Symantec Research Labs
Pierre-Antoine_Vervier@symantec.com

Disclaimer

- In this presentation, for the sake of conciseness, we talk about hijacks and attacker instead of candidate hijacks and likely attacker even though we have no bullet proof evidence of their wrong doing.
- IP address blocks and ASes were likely abused in hijacks between January 2013 and June 2014 and, therefore, might now be legitimately used.