BAD ASN - A BGP Hijack Research

Chunhui Gao / Yu Guo

IPIP

Company Overview

- IP Intelligence company
    - ASN/ BGP, Geo location research and product.

- We serve more than 80% of top 100 internet companies in China;

- With clients in Asia, EU and North America
    - User profiling, CDN, DNS, DDoS mitigation
    - Threat intelligence, Anti-fraud.
    - Proxy detection
    - Advertising
    - Geo fencing

History of BGP Hijack

- BGP is lacking of validation during BGP Announcement
  - IRR, RPKI, MANRS: Not enough.
- Prefix Hijacking
  - Announce ANY prefix under an specific ASN

- Common Techniques in BGP Hijacking History
  - Human Typo
    - Feb 2008, Pakistan Telecom hijacked Youtube
  - For Profit:
    - Apr 2018, Hijack Amazon DNS to take over Crypto MyEtherWallet
  - Long term Hijacking (aka. BAD ASN by IPIP.net)
    - Extremely hidden
    - SPAM/ DDoS/ Web Scraping/ Proxy

How do we find BAD ASN?

- ASN/ BGP data is important source for us to make IP data correct.
  - We created our own BGP data and tools to monitor

- ASN IP prefix and Up/ Downstream Changes
  - Especially these Suspicious Announcement Issue
    - Prefix is announced in different locations
    - Prefix is announced and withdrawn in hours or days from same ASN

- Data conflicts in ASN and Prefix

BAD ASN – The Hidden Hijacking

- IP Prefix Theft/ Abuse
    - Announce prefixes that not in use. (It will show in Geo comparison with origin ASN)
    - Usually withdrawn in days
    - Mixed with normal prefix to avoid detection.

- ASN Theft/ Abuse

- Downstream of BAD ASN are almost 100% BAD.
- Mixed with normal prefix to avoid detection.

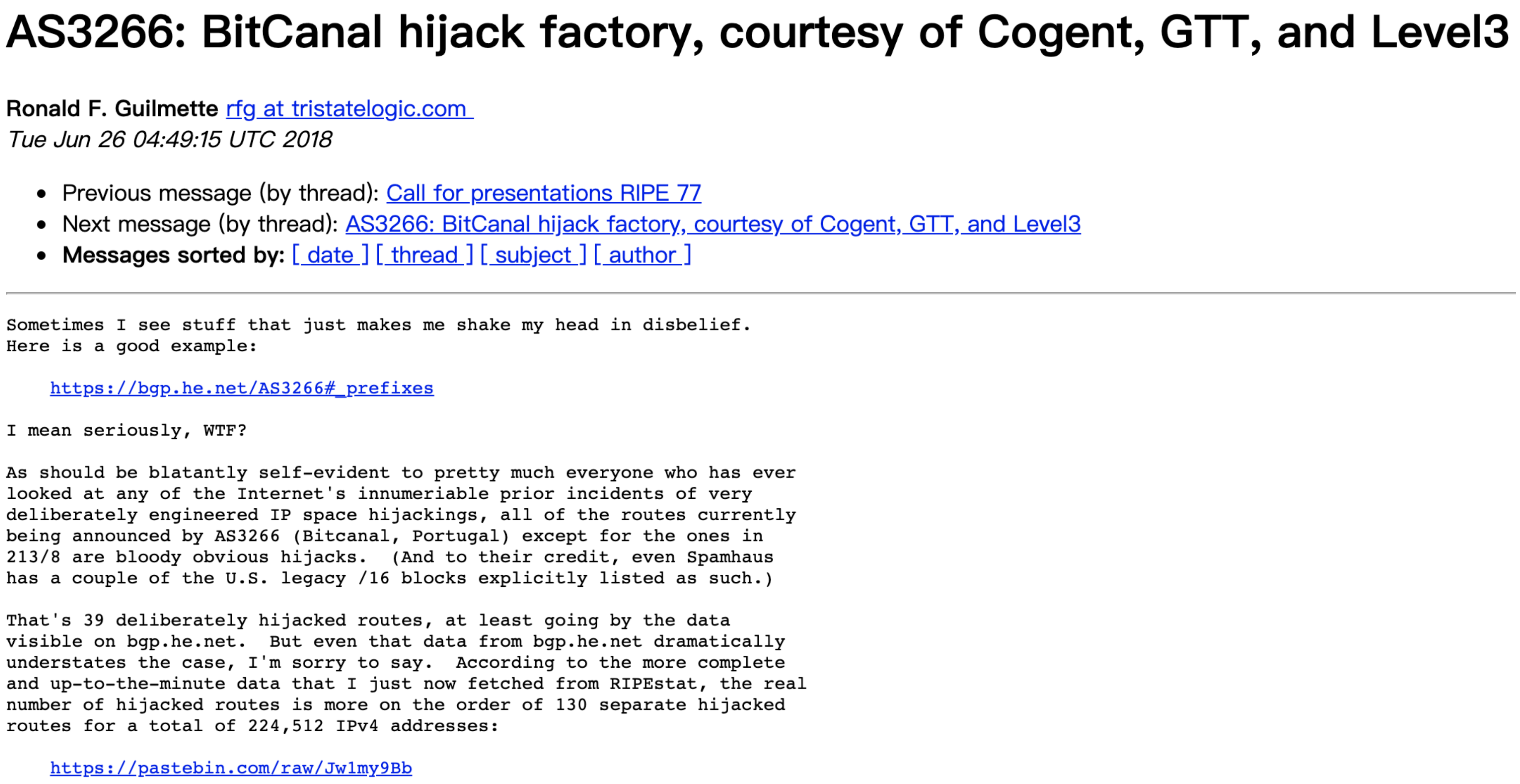
Purpose of BAD ASN

- SPAM
  - Snowshoe SPAM Attack
- Proxy Service
- Spider/ Crawler Farm
- Other Abuse?

Case Study

- https://mailman.nanog.org/pipermail/nanog/2018-June/096034.html
- https://dyn.com/blog/shutting-down-the-bgp-hijack-factory/
- https://mailman.nanog.org/pipermail/nanog/2018-July/096437.html

BitCanal Hijack



AS3266: BitCanal hijack factory, courtesy of Cogent, GTT, and Level3

Ronald F. Guilmette rfg at tristatelogic.com
Tue Jun 26 04:49:15 UTC 2018

- Previous message (by thread): Call for presentations RIPE 77
- Next message (by thread): AS3266: BitCanal hijack factory, courtesy of Cogent, GTT, and Level3
- **Messages sorted by:** [date] [thread] [subject] [author]

Sometimes I see stuff that just makes me shake my head in disbelief.
Here is a good example:

    https://bgp.he.net/AS3266#_prefixes

I mean seriously, WTF?

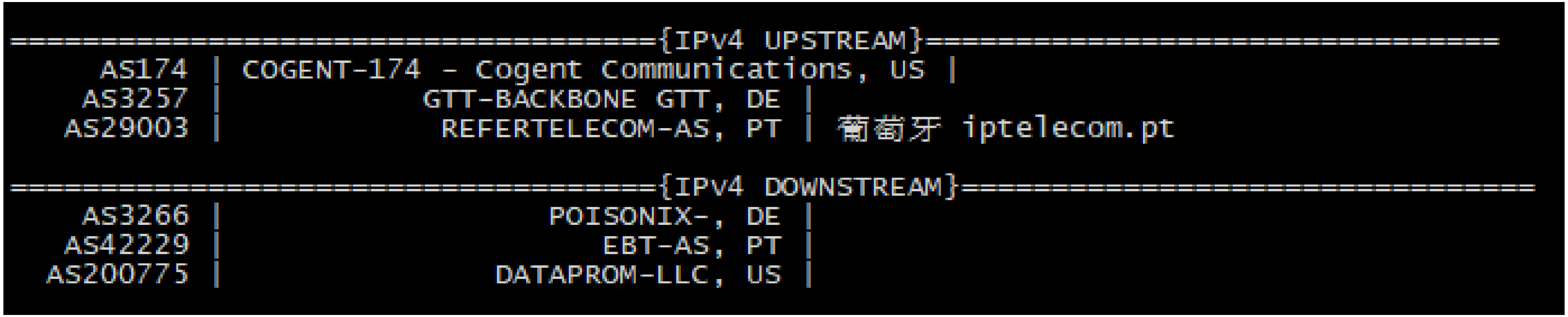
As should be blatantly self-evident to pretty much everyone who has ever looked at any of the Internet's innumeriable prior incidents of very deliberately engineered IP space hijackings, all of the routes currently being announced by AS3266 (Bitcanal, Portugal) except for the ones in 213/8 are bloody obvious hijacks. (And to their credit, even Spamhaus has a couple of the U.S. legacy /16 blocks explicitly listed as such.)

That's 39 deliberately hijacked routes, at least going by the data visible on bgp.he.net. But even that data from bgp.he.net dramatically understates the case, I'm sorry to say. According to the more complete and up-to-the-minute data that I just now fetched from RIPEstat, the real number of hijacked routes is more on the order of 130 separate hijacked routes for a total of 224,512 IPv4 addresses:

    https://pastebin.com/raw/Jw1my9Bb

BitCanal SPAM

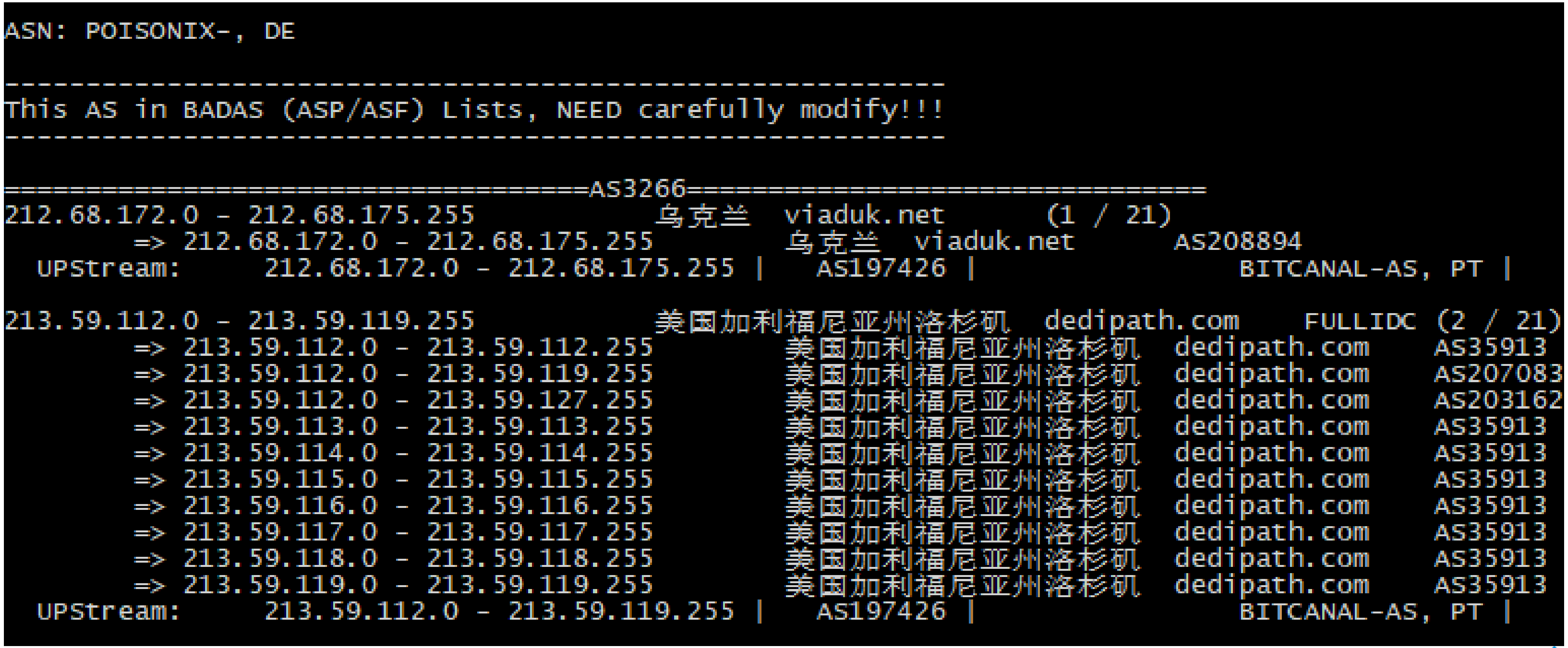
- Up/ Downstream of AS197426
  - Focus on downstream



```
===================================={IPv4 UPSTREAM}===============================
     AS174 | COGENT-174 - Cogent Communications, US |
    AS3257 |          GTT-BACKBONE GTT, DE |
   AS29003 |           REFERTELECOM-AS, PT | 葡萄牙 iptelecom.pt

===================================={IPv4 DOWNSTREAM}===============================
    AS3266 |                 POISONIX-, DE |
   AS42229 |                    EBT-AS, PT |
  AS200775 |              DATAPROM-LLC, US |
```

BitCanal SPAM

- ASN 3266
  - Many California Prefixes announced/ Hijacked in DE ASN
  - Origin prefix owner to announce /24 to mitigate Hijacking.



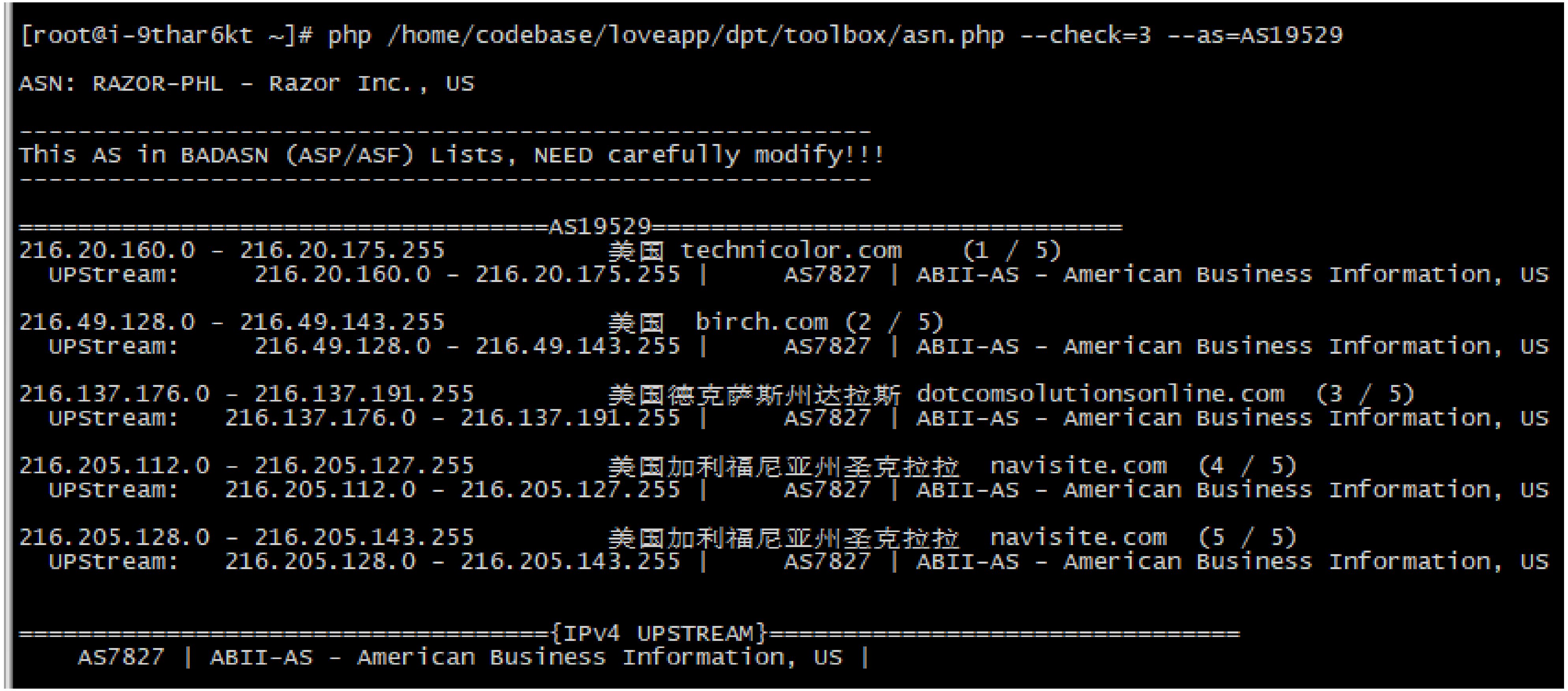
```
ASN: POISONIX-, DE

----------------------------------------------------------
This AS in BADAS (ASP/ASF) Lists, NEED carefully modify!!!
----------------------------------------------------------

====================================AS3266====================================
212.68.172.0 - 212.68.175.255          乌克兰  viaduk.net      (1 / 21)
        => 212.68.172.0 - 212.68.175.255        乌克兰  viaduk.net      AS208894
  UPStream:     212.68.172.0 - 212.68.175.255 |   AS197426 |               BITCANAL-AS, PT |

213.59.112.0 - 213.59.119.255          美国加利福尼亚州洛杉矶  dedipath.com    FULLIDC (2 / 21)
        => 213.59.112.0 - 213.59.112.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.112.0 - 213.59.119.255        美国加利福尼亚州洛杉矶  dedipath.com    AS207083
        => 213.59.112.0 - 213.59.127.255        美国加利福尼亚州洛杉矶  dedipath.com    AS203162
        => 213.59.113.0 - 213.59.113.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.114.0 - 213.59.114.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.115.0 - 213.59.115.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.116.0 - 213.59.116.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.117.0 - 213.59.117.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.118.0 - 213.59.118.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
        => 213.59.119.0 - 213.59.119.255        美国加利福尼亚州洛杉矶  dedipath.com    AS35913
  UPStream:     213.59.112.0 - 213.59.119.255 |   AS197426 |               BITCANAL-AS, PT |
```

More BAD ASN examples:

- AS205869 - Universal IP Solution Corp., UA
    - AS7827 - American Business Information, US
        - AS19529 - Razor Inc., US
    - AS11717 – Solarus,US
        - AS10800 - Internet Arena, US

More BAD ASN examples:

- AS205869 - Universal IP Solution Corp., UA
    - AS7827 - American Business Information, US

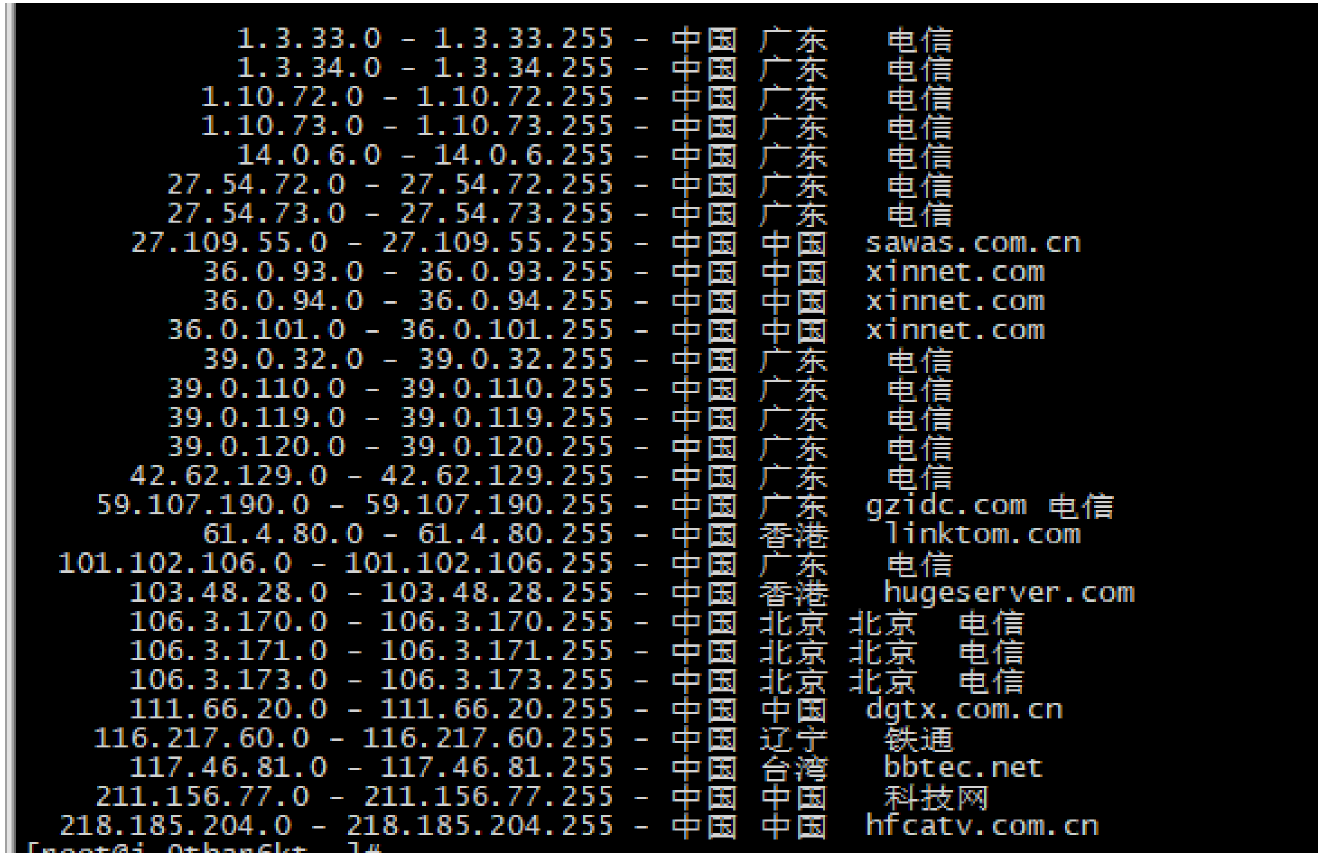


```
[root@i-9thar6kt ~]# php /home/codebase/loveapp/dpt/toolbox/asn.php --check=3 --as=AS19529

ASN: RAZOR-PHL - Razor Inc., US

----------------------------------------------------------
This AS in BADASN (ASP/ASF) Lists, NEED carefully modify!!!
----------------------------------------------------------

====================================AS19529================================
216.20.160.0 - 216.20.175.255           美国 technicolor.com    (1 / 5)
  UPstream:     216.20.160.0 - 216.20.175.255 |     AS7827 | ABII-AS - American Business Information, US

216.49.128.0 - 216.49.143.255           美国  birch.com (2 / 5)
  UPstream:     216.49.128.0 - 216.49.143.255 |     AS7827 | ABII-AS - American Business Information, US

216.137.176.0 - 216.137.191.255         美国德克萨斯州达拉斯 dotcomsolutionsonline.com  (3 / 5)
  UPstream:   216.137.176.0 - 216.137.191.255 |     AS7827 | ABII-AS - American Business Information, US

216.205.112.0 - 216.205.127.255         美国加利福尼亚州圣克拉拉  navisite.com  (4 / 5)
  UPstream:   216.205.112.0 - 216.205.127.255 |     AS7827 | ABII-AS - American Business Information, US

216.205.128.0 - 216.205.143.255         美国加利福尼亚州圣克拉拉  navisite.com  (5 / 5)
  UPstream:   216.205.128.0 - 216.205.143.255 |     AS7827 | ABII-AS - American Business Information, US


===================================={IPv4 UPSTREAM}================================
    AS7827 | ABII-AS - American Business Information, US |
```

Case in APAC

- AS133741
- HONGKONG YABOIDC TECHNOLOGY LIMITED

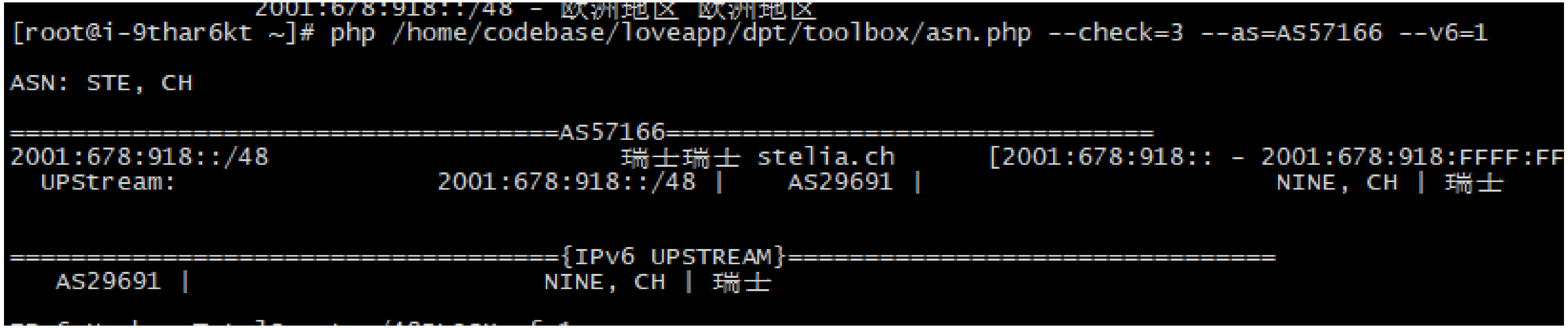
- Upstream
- AS3491 – PCCW
- AS18046 - DongFong Technology Co. Ltd., TW



```
          1.3.33.0 - 1.3.33.255 - 中国 广东   电信
          1.3.34.0 - 1.3.34.255 - 中国 广东   电信
        1.10.72.0 - 1.10.72.255 - 中国 广东   电信
        1.10.73.0 - 1.10.73.255 - 中国 广东   电信
          14.0.6.0 - 14.0.6.255 - 中国 广东   电信
      27.54.72.0 - 27.54.72.255 - 中国 广东   电信
      27.54.73.0 - 27.54.73.255 - 中国 广东   电信
    27.109.55.0 - 27.109.55.255 - 中国 中国  sawas.com.cn
        36.0.93.0 - 36.0.93.255 - 中国 中国  xinnet.com
        36.0.94.0 - 36.0.94.255 - 中国 中国  xinnet.com
      36.0.101.0 - 36.0.101.255 - 中国 中国  xinnet.com
        39.0.32.0 - 39.0.32.255 - 中国 广东   电信
      39.0.110.0 - 39.0.110.255 - 中国 广东   电信
      39.0.119.0 - 39.0.119.255 - 中国 广东   电信
      39.0.120.0 - 39.0.120.255 - 中国 广东   电信
    42.62.129.0 - 42.62.129.255 - 中国 广东   电信
  59.107.190.0 - 59.107.190.255 - 中国 广东  gzidc.com 电信
        61.4.80.0 - 61.4.80.255 - 中国 香港   linktom.com
101.102.106.0 - 101.102.106.255 - 中国 广东   电信
    103.48.28.0 - 103.48.28.255 - 中国 香港   hugeserver.com
    106.3.170.0 - 106.3.170.255 - 中国 北京 北京  电信
    106.3.171.0 - 106.3.171.255 - 中国 北京 北京  电信
    106.3.173.0 - 106.3.173.255 - 中国 北京 北京  电信
    111.66.20.0 - 111.66.20.255 - 中国 中国  dgtx.com.cn
  116.217.60.0 - 116.217.60.255 - 中国 辽宁   铁通
    117.46.81.0 - 117.46.81.255 - 中国 台湾   bbtec.net
  211.156.77.0 - 211.156.77.255 - 中国 中国   科技网
218.185.204.0 - 218.185.204.255 - 中国 中国  hfcatv.com.cn
```

BAD ASN in IPv6

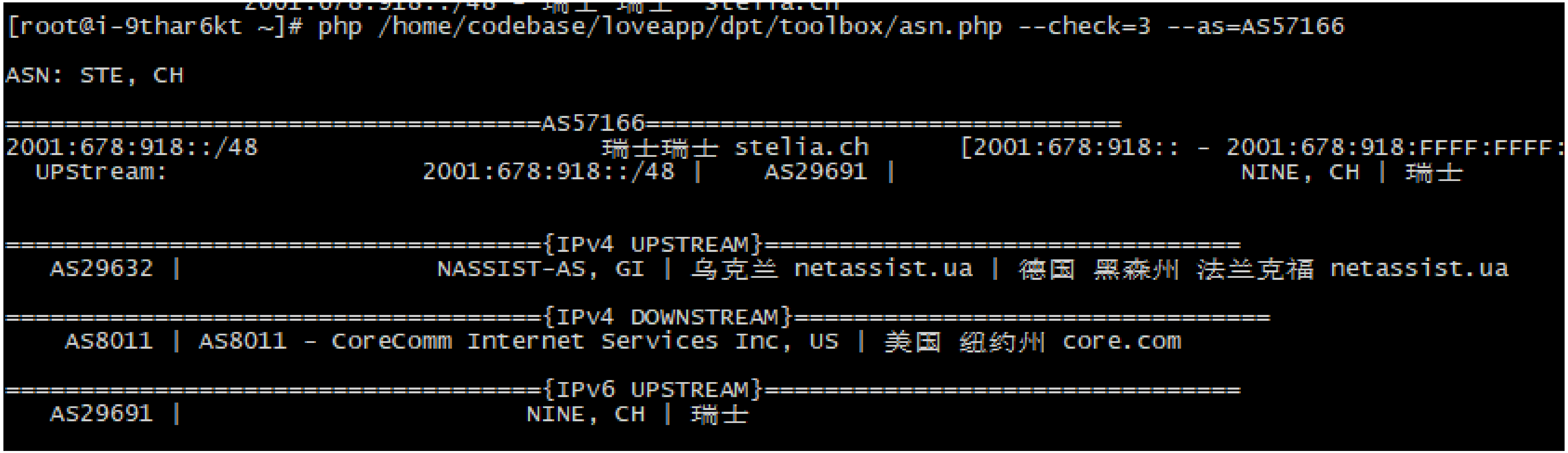
- AS57166 in Switzerland



```
                2001:678:918::/48 - 欧洲地区 欧洲地区
[root@i-9thar6kt ~]# php /home/codebase/loveapp/dpt/toolbox/asn.php --check=3 --as=AS57166 --v6=1

ASN: STE, CH

====================================AS57166================================
2001:678:918::/48                       瑞士瑞士 stelia.ch     [2001:678:918:: - 2001:678:918:FFFF:FF
  UPStream:                 2001:678:918::/48 |    AS29691 |                      NINE, CH | 瑞士


===================================={IPv6 UPSTREAM}================================
   AS29691 |                       NINE, CH | 瑞士
```

BAD ASN in IPv6

- AS57166 in Switzerland
  - Comparison with IPv4 data



```
                2001:678:918::/48 - 瑞士 瑞士  stelia.ch
[root@i-9thar6kt ~]# php /home/codebase/loveapp/dpt/toolbox/asn.php --check=3 --as=AS57166

ASN: STE, CH

====================================AS57166================================
2001:678:918::/48                        瑞士瑞士 stelia.ch      [2001:678:918:: - 2001:678:918:FFFF:FFFF:
  UPStream:                 2001:678:918::/48 |     AS29691 |                       NINE, CH | 瑞士


===================================={IPv4 UPSTREAM}================================
   AS29632 |                 NASSIST-AS, GI | 乌克兰 netassist.ua | 德国 黑森州 法兰克福 netassist.ua

===================================={IPv4 DOWNSTREAM}================================
    AS8011 | AS8011 - CoreComm Internet Services Inc, US | 美国 纽约州 core.com

===================================={IPv6 UPSTREAM}================================
   AS29691 |                       NINE, CH | 瑞士
```

BAD ASN – Summary

- IP Prefix Theft/ Abuse
  - Announce prefixes that not in use. (It will show in Geo comparison with origin ASN)
  - Usually withdrawn in days
  - Mixed with normal prefix to avoid detection.

- ASN Theft/ Abuse

- Downstream of BAD ASN are almost 100% BAD.
- Mixed with normal prefix to avoid detection.

About asndrop.txt of Spamhaus.org

- ASN LIST will bring false positives.
- Not a perfect solution to block all prefixes in the same ASN.
- ASN Theft Issues.

Suggestion

- Announce & Monitor all your IP prefixes.
- Announce & Monitor all your ASNs.
- What to do if any abuse detected:
    - Announce your prefix with /24 or smaller
    - contact abuse@ISP or its upstream providers.

Questions?