



BackConnect's Suspicious BGP Hijacks

Doug Madory
NANOG 68
Dallas, Texas

INTERNET
PERFORMANCE.
DELIVERED.

 dyn.com  [@dyn](https://twitter.com/dyn)



08 Israeli Online Attack Service 'vDOS' Earned \$600,000 in Two Years

SEP 16

vDOS — a “booter” service that has earned in excess of \$600,000 over the past two years helping customers coordinate more than 150,000 so-called distributed denial-of-service (DDoS) attacks designed to knock Web sites offline — has been massively hacked, spilling secrets about tens of thousands of paying customers and their targets.

The vDOS database, obtained by KrebsOnSecurity.com at the end of July 2016, points to two young men in Israel as the principal owners and masterminds of the attack service, with support services coming from several young hackers in the United States.



vDOS



How do I purchase a vDos plan?

Purchasing a booter plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

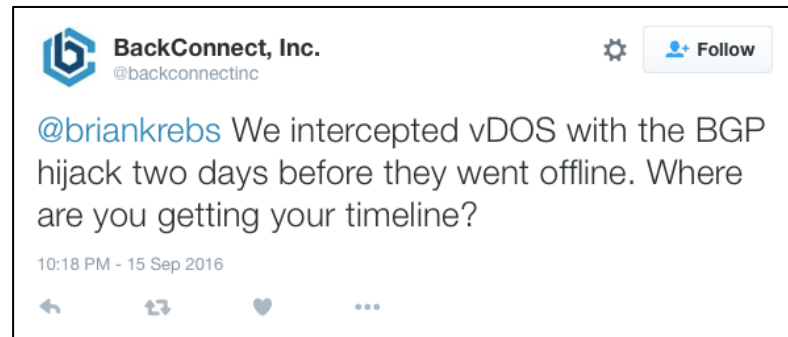


BackConnect Admits to BGP Hijack of vDOS

- BackConnect CEO confirms BGP hijack was done, but it was for 'defensive purposes'
- *Perhaps first time perpetrator of a BGP hijack confirms act intended for interception.*



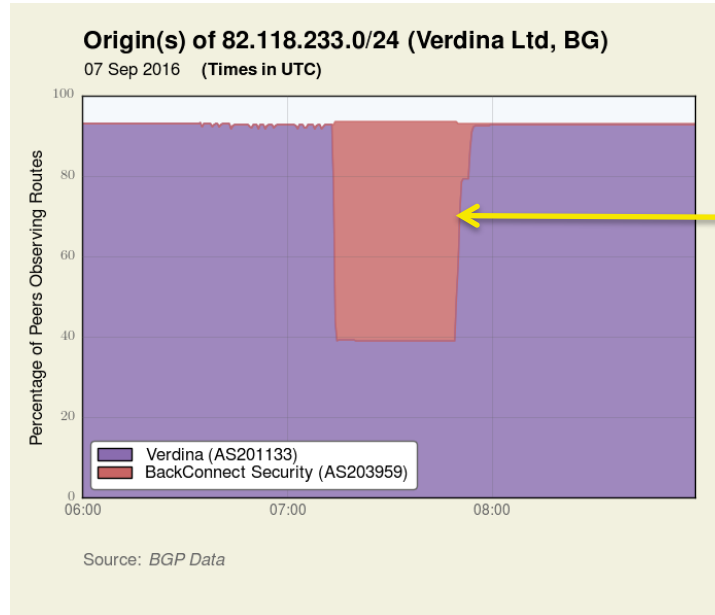
A screenshot of a tweet from user @briankrebs. The tweet text reads: "Alleged co-owners of attack-for-hire site vDOS arrested in Israel. CEO of a victim company admits to BGP hijacking krebsonsecurity.com/2016/09/allege...". The tweet has 230 retweets and 215 likes. It was posted at 3:15 PM on 10 Sep 2016. The user's profile picture is a small square image of a man, and the name is "briankrebs" with a verified badge. A "Following" button is visible in the top right corner of the tweet card.



A screenshot of a tweet from BackConnect, Inc. (@backconnectinc). The tweet text reads: "@briankrebs We intercepted vDOS with the BGP hijack two days before they went offline. Where are you getting your timeline?". The tweet was posted at 10:18 PM on 15 Sep 2016. The user's profile picture is a blue hexagonal logo with a white 'b', and the name is "BackConnect, Inc." with a verified badge. A "Follow" button is visible in the top right corner of the tweet card.

BackConnect Hijack of Verdina (vDOS)

- BackConnect (AS203959) began announcing 82.118.233.0/24 (Verdina Ltd.) at 07:13:26 UTC on 7 Sep 2016
- > Half of our peers accepted hijacked BGP route for ~50 minutes



BackConnect hijack

BackConnect Hijack of Verdina (vDOS)

- Example traceroute to Verdina (Sofia, BG) before hijack

trace from AWS Ashburn, VA to 82.118.233.12 at 08:19 Sep 06, 2016

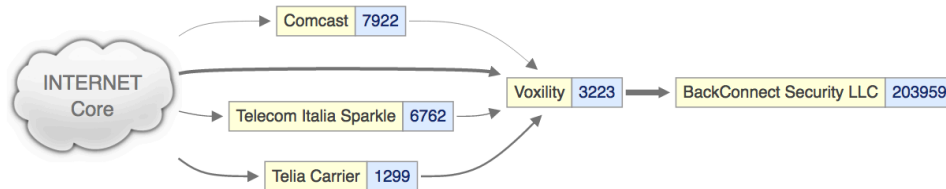
```
1 *
2 *
3 100.65.11.65    RFC 6598 (carrier-grade NAT)                0.589
4 205.251.245.227 Amazon.com, Inc.                            Ashburn    US    1.421
5 54.239.110.24  Amazon Technologies Inc.                     Ashburn    US    1.468
6 54.239.110.7   Amazon Technologies Inc.                     Ashburn    US    1.491
7 67.133.224.193 dca2-edge-02.inet.qwest.net                  Washington US    2.009
8 67.14.28.18   dcp-brdr-04.inet.qwest.net                  Washington US    2.554
9 154.54.11.129  be3045.ccr41.iad02.atlas.cogentco.com        Washington US    1.878
10 154.54.31.109 be2657.ccr42.dca01.atlas.cogentco.com        Washington US    3.104
11 154.54.40.109  be2807.ccr42.jfk02.atlas.cogentco.com        New York   US    9.058
12 154.54.42.86   be2490.ccr42.lon13.atlas.cogentco.com        London     GB    77.922
13 130.117.51.42  be12488.ccr42.ams03.atlas.cogentco.com        Amsterdam  NL    83.648
14 130.117.0.142  be2814.ccr42.fra03.atlas.cogentco.com        Frankfurt  DE    93.298
15 154.54.36.254  be2960.ccr22.muc03.atlas.cogentco.com        Munich     DE    100.592
16 154.54.58.14   be2975.ccr21.vie01.atlas.cogentco.com        Vienna     AT    104.828
17 130.117.1.21   be2046.ccr21.sof02.atlas.cogentco.com        Sofia      BG    125.216
18 *
```

BackConnect Hijack of Verdina (vDOS)

- Example traceroute to Verdina (Sofia, BG) during hijack

trace from AWS Ashburn, VA to 82.118.233.12 at 07:41 Sep 07, 2016

```
1 *
2 *
3 100.65.11.65    RFC 6598 (carrier-grade NAT)           0.478
4 205.251.245.184 Amazon.com, Inc.                      Ashburn    US    0.668
5 54.239.111.10  Amazon Technologies Inc.              Ashburn    US    1.054
6 54.239.108.209 Amazon Technologies Inc.              Ashburn    US    0.75
7 50.242.148.69  Comcast Cable Communications, LL       Ashburn    US    1.436
8 173.167.58.130 Comcast Business Communications,       Ashburn    US    1.12
9 37.221.173.74  ash-eqx-01c.voxility.net              Ashburn    US    1.283
10 5.254.109.90   lax-eqx-01c.voxility.net              Los Angeles US    62.358
11 82.118.233.12  Verdina Ltd.                           62.633
```



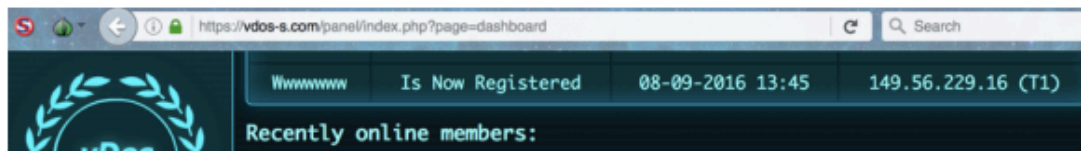


20 DDoS Mitigation Firm Has History of Hijacks

SEP 16

Last week, KrebsOnSecurity detailed how **BackConnect Inc.** — a company that defends victims against large-scale distributed denial-of-service (DDoS) attacks — admitted to hijacking hundreds of Internet addresses from a European Internet service provider in order to glean information about attackers who were targeting BackConnect. According to an exhaustive analysis of historic Internet records, BackConnect appears to have a history of such “hacking back” activity.

On Sept. 8, 2016, KrebsOnSecurity **exposed the inner workings of vDOS**, a DDoS-for-hire or “booter” service whose tens of thousands of paying customers used the service to launch attacks against hundreds of thousands of targets over the service’s four-year history in business.

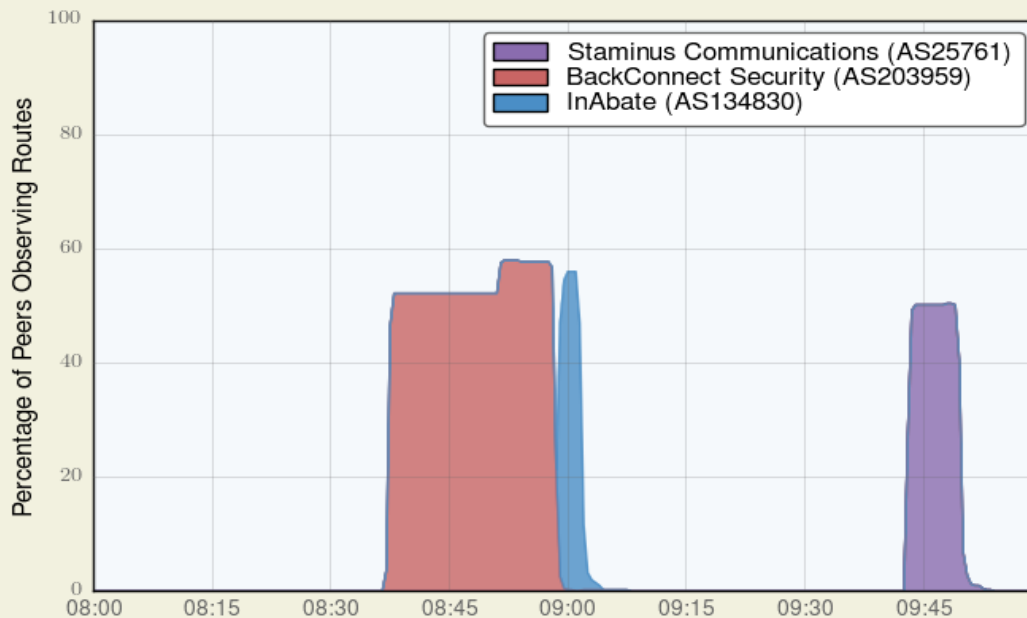


My New Book!

BackConnect Hijack of Staminus

Origins of 72.20.0.0/24 (Staminus)

20 Feb 2016 (Times in UTC)



Source: BGP Data

BackConnect Hijack of Staminus

Origins of 72.20.0.0/24 (Staminus)

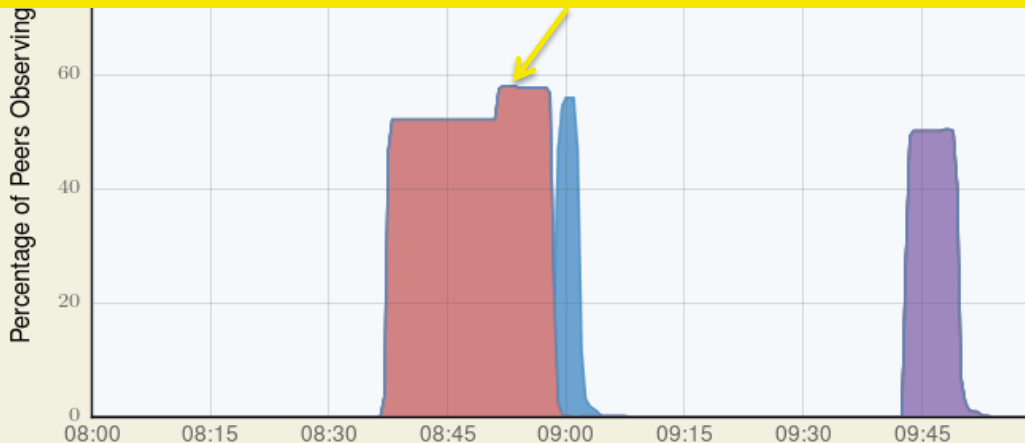
20 Feb 2016 (Times in UTC)

100

3223=Voxility
203959=BackConnect

- At 08:36:59 UTC on 20 February 2016, BackConnect began hijacking using the following AS path:

... 3223 203959 53587 53587 53587 53587 134830 134830 134830 203959 203959



Source: BGP Data

53587=CloudDDoS
134830=InAbate

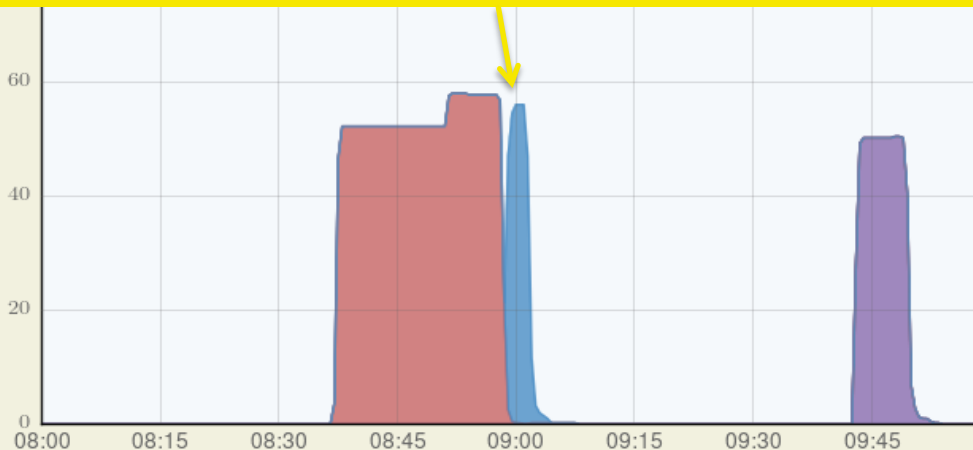
BackConnect Hijack of Staminus

Origins of 72.20.0.0/24 (Staminus)

20 Feb 2016 (Times in UTC)

100

Percentage of Peers Observing



Source: BGP Data

3223=Voxility
203959=BackConnect

- Then the AS path changed to following with InAbate (AS134830) ostensibly as the origin:

... 3223 203959 32768 53587 53587 53587 53587 134830 134830 134830

53587=CloudDDoS
134830=InAbate

BackConnect Hijack of Staminus

Origins of 72.20.0.0/24 (Staminus)

20 Feb 2016 (Times in UTC)

100

Percentage of Peers Observing

60
40
20
0

08:00 08:15 08:30 08:45 09:00 09:15 09:30 09:45

Source: BGP Data

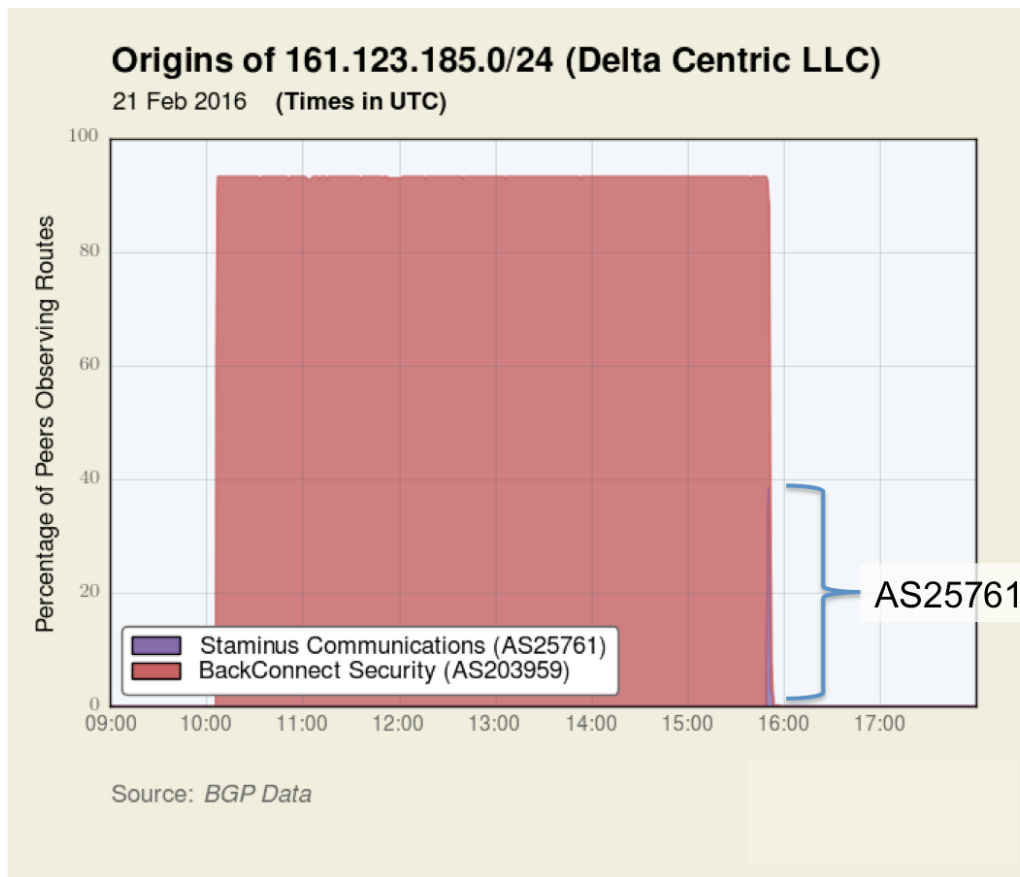
3223=Voxility
203959=BackConnect

- Finally, BackConnect added AS25761 (Staminus) as the origin, taking the form:

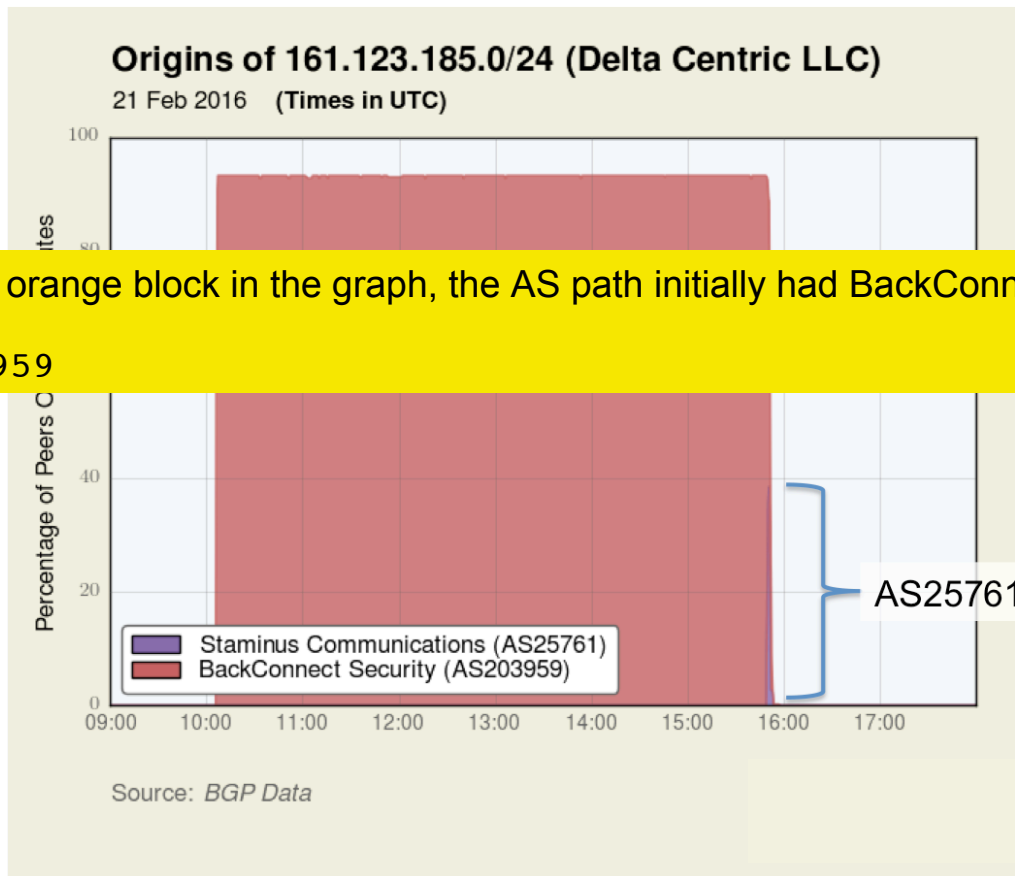
... 3223 203959 1229 3257 25761

- 3257 (GTT) and 1299 (Telia) are providers of Staminus

BackConnect Hijack of GhostNet route



BackConnect Hijack of GhostNet route

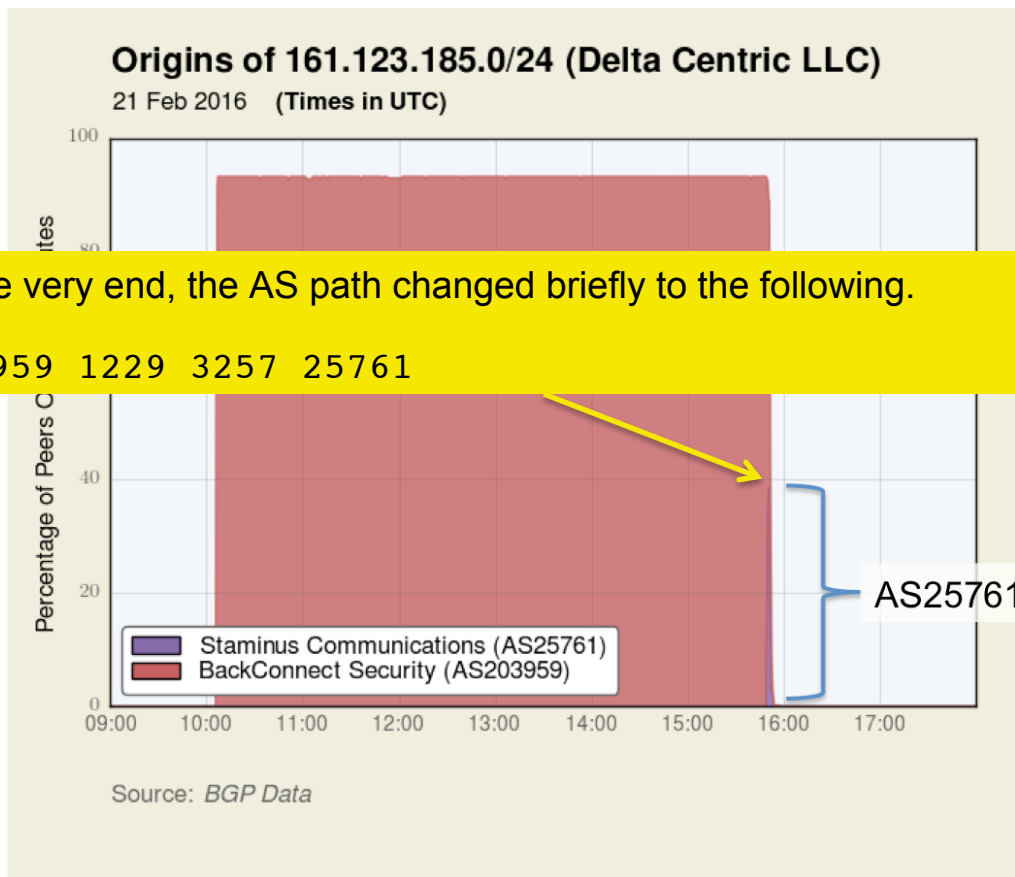


3223=Voxility
203959=BackConnect

- During the orange block in the graph, the AS path initially had BackConnect as the origin:

... 3223 203959

BackConnect Hijack of GhostNet route



3223=Voxility
203959=BackConnect

- Then at the very end, the AS path changed briefly to the following.

... 3223 203959 1229 3257 25761

- 3257 (GTT) and 1299 (Telia) are providers of Staminus

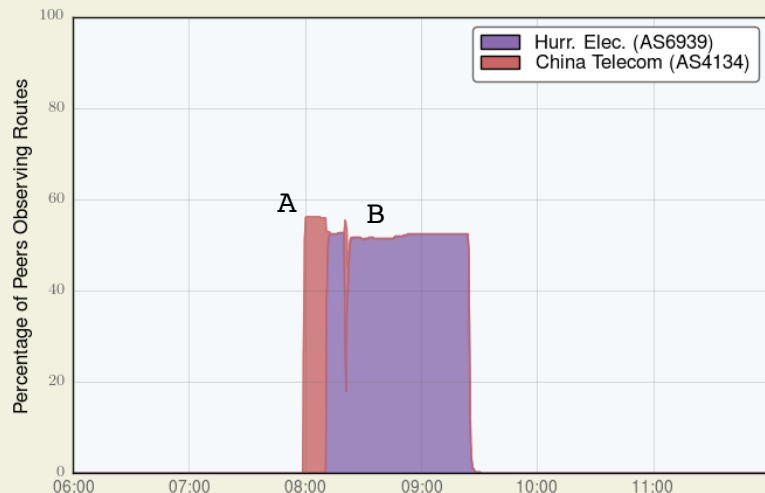
More forged AS paths by BackConnect

A) ... 3223 203959 4134

B) ... 3223 203959 4134 42708 36236 6939

Origin(s) of 146.84.2.0/24 (Tivoli Systems)

21 Feb 2016 (Times in UTC)



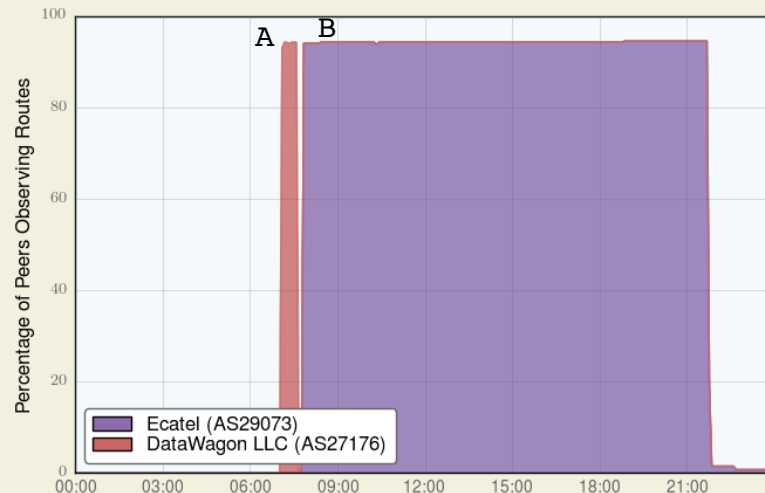
Source: BGP Data

A) ... 3223 203959 27176

B) ... 3223 203959 29073

Origins of 161.123.172.0/24 (Tesonet,DE)

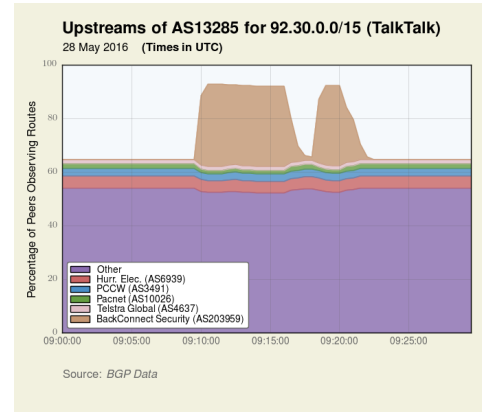
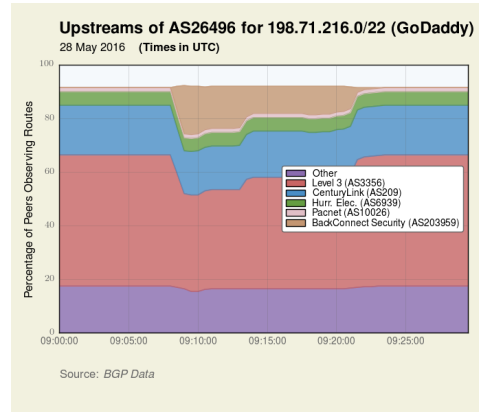
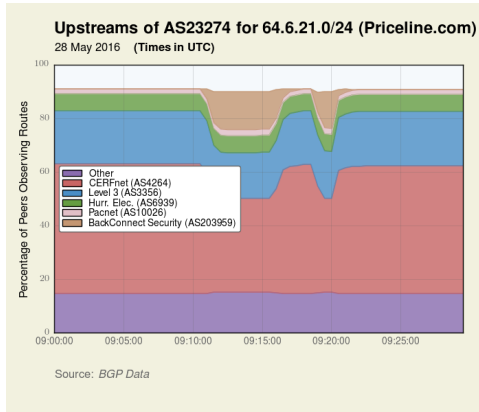
16 Apr 2016 - 17 Apr 2016 (Times in UTC)



Source: BGP Data

BackConnect's Routing Leak?

- On 28 May, BackConnect announced >13,000 routes via Voxility.
- Traffic briefly re-directed through Voxility (and BackConnect?) during leak.



Summary

- BackConnect is first security company to confirm its use of BGP hijack to intercept traffic
- Previous hijacks suggest that this wasn't the first time BackConnect did this (CEO blames previous hijacks on former employee)
- As additional BGP-based DDoS mitigation companies enter the market, more entities announcing others' space
- *Question for NANOG community...*

A globe is shown in the background, partially obscured by a complex network of white lines and nodes, representing a global network or data flow. The globe is dark, and the network lines are bright white. The overall background is black, with a yellow curved shape at the bottom.

Could there ever be a scenario in which using BGP to hijack another's IP space be *justifiable*?

Epilog



briankrebs ✓

@briankrebs

 Follow

Holy moly. Prolexic reports my site was just hit with the largest DDOS the internet has ever seen. 665 Gbps. Site's still up. #FAIL

3:02 AM - 21 Sep 2016



THANK YOU!



DynSM

INTERNET PERFORMANCE. **DELIVERED.**

Doug Madory

dmadory@dyn.com

[@dynresearch](https://twitter.com/dynresearch)



dyn.com [@dyn](https://twitter.com/dyn)