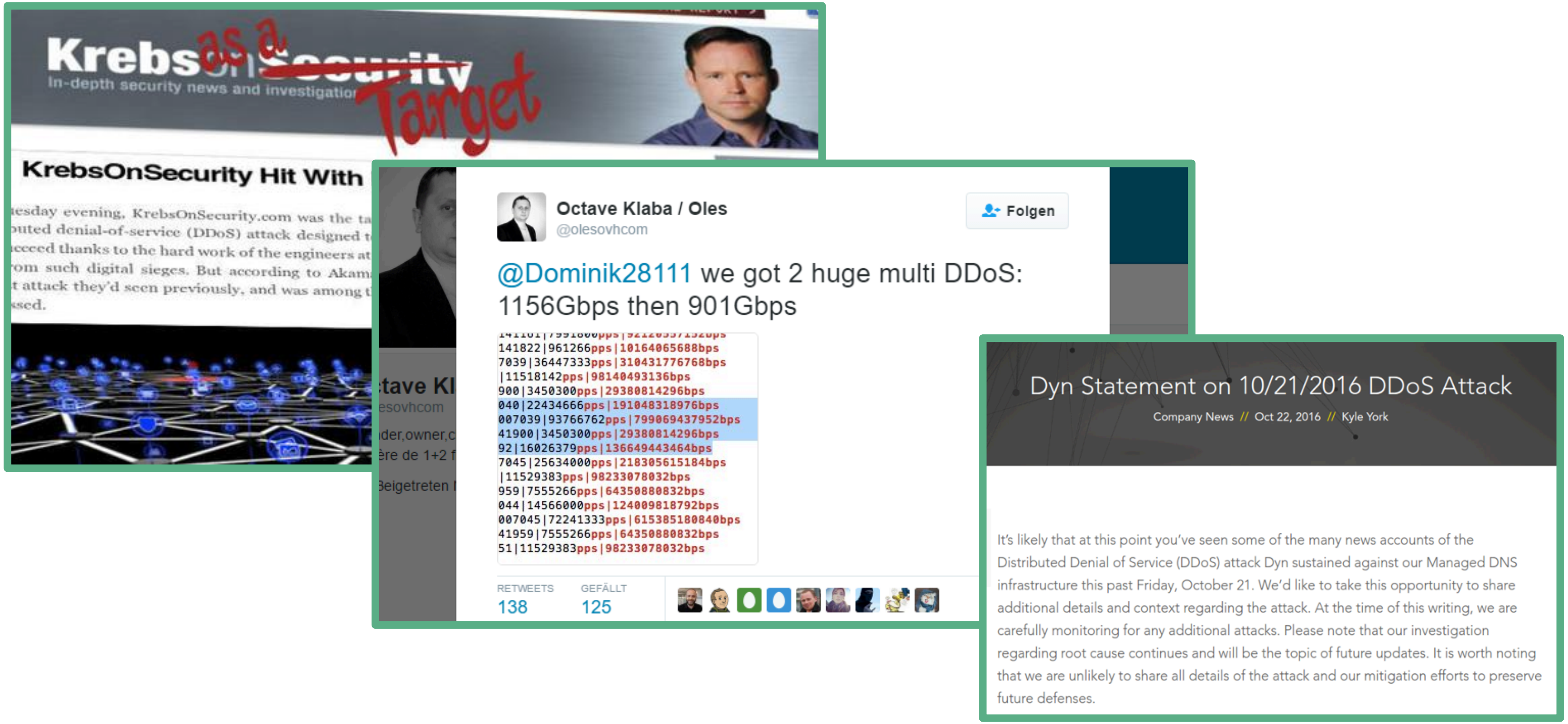
Inferring BGP Blackholing Activity in the Internet

NANOG 72, Atlanta

Vasileios Giotsas [†*], Georgios Smaragdakis [‡†], **Christoph Dietzel** [†§], Philipp Richter [†], Anja Feldmann [†], Arthur Berger [¶‡]

[†]TU Berlin [*]CAIDA [§]DE-CIX [‡]MIT [¶]Akamai

Motivation



Krebs ~~on Security~~ as a Target
In-depth security news and investigation

KrebsOnSecurity Hit With

uesday evening, KrebsOnSecurity.com was the ta
buted denial-of-service (DDoS) attack designed t
ucceed thanks to the hard work of the engineers at
rom such digital sieges. But according to Akam
t attack they'd seen previously, and was among t
ssed.

Octave Klaba / Oles
@olesovhcom

@Dominik28111 we got 2 huge multi DDoS: 1156Gbps then 901Gbps

```
141161|7991800pps|92120557152bps
141822|961266pps|10164065688bps
7039|36447333pps|310431776768bps
|11518142pps|98140493136bps
900|3450300pps|29380814296bps
040|22434666pps|191048318976bps
007039|93766762pps|799069437952bps
41900|3450300pps|29380814296bps
92|16026379pps|136649443464bps
7045|25634000pps|218305615184bps
|11529383pps|98233078032bps
959|7555266pps|64350880832bps
044|14566000pps|124009818792bps
007045|72241333pps|615385180840bps
41959|7555266pps|64350880832bps
51|11529383pps|98233078032bps
```

RETWEETS 138 GEFÄLLT 125

ctave Kl
esovhcom
nder,owner,c
ère de 1+2 f
Beigetreten

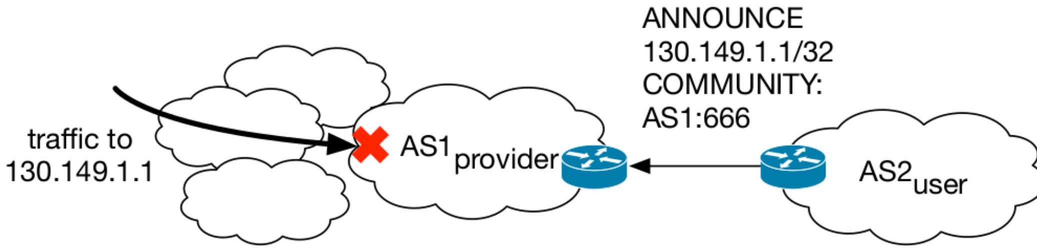
Dyn Statement on 10/21/2016 DDoS Attack

Company News // Oct 22, 2016 // Kyle York

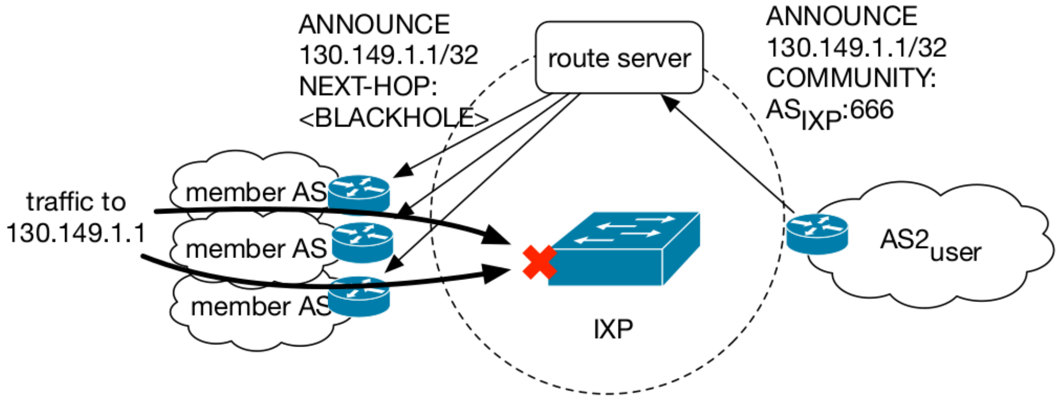
It's likely that at this point you've seen some of the many news accounts of the Distributed Denial of Service (DDoS) attack Dyn sustained against our Managed DNS infrastructure this past Friday, October 21. We'd like to take this opportunity to share additional details and context regarding the attack. At the time of this writing, we are carefully monitoring for any additional attacks. Please note that our investigation regarding root cause continues and will be the topic of future updates. It is worth noting that we are unlikely to share all details of the attack and our mitigation efforts to preserve future defenses.

Blackholing

Blackholing [RFC1997, RFC7999]



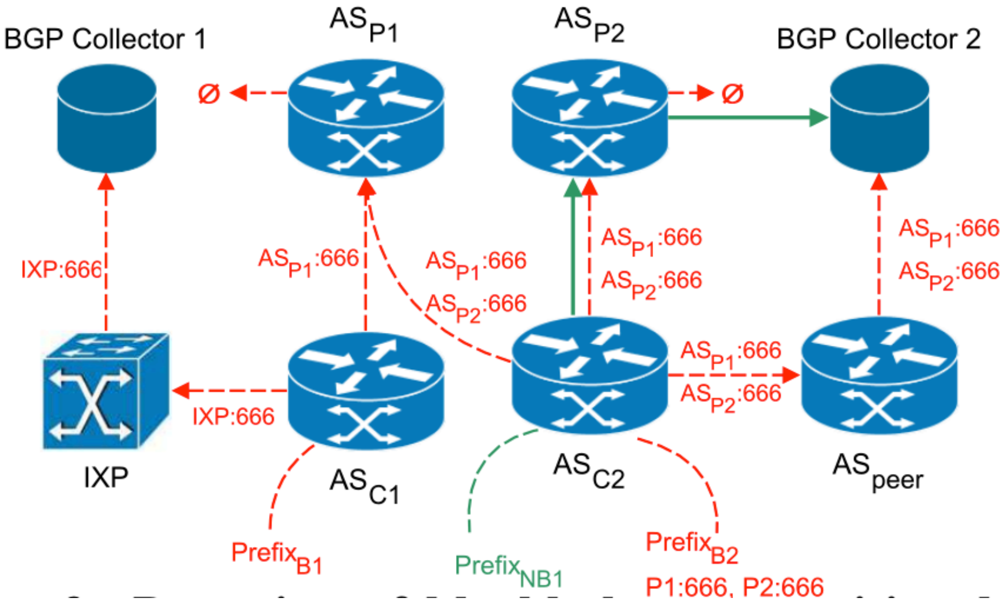
Blackholing at IXPs



Research Goals

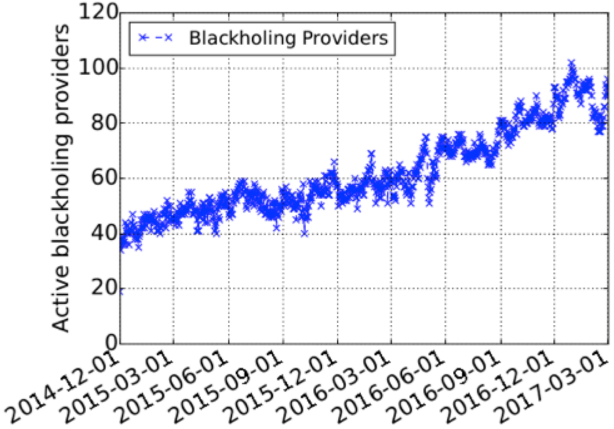
- Internet wide-adoption
- Profile the targets using blackholing
- Blackholing practices
- Network efficacy

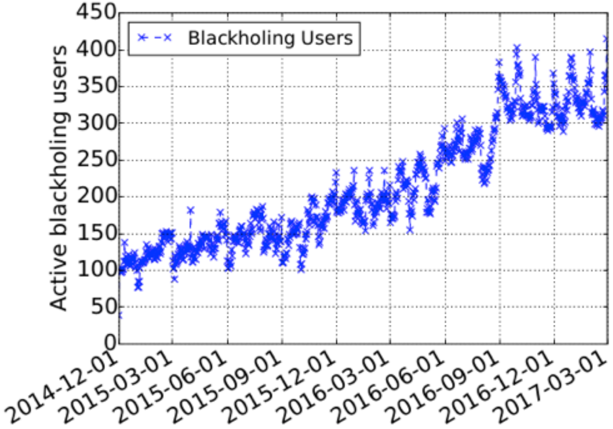
Blackhole Communities, Vantage Points

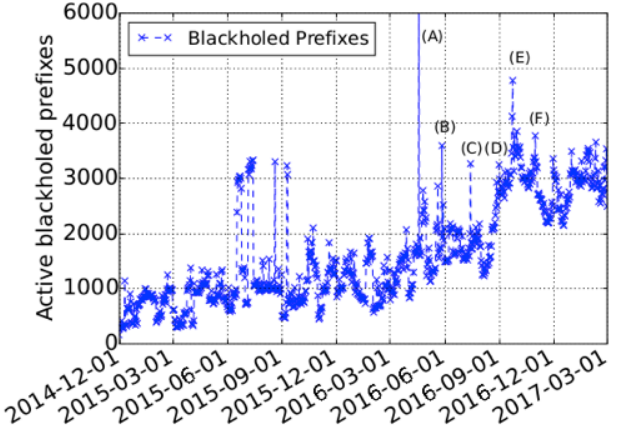


Inferring BGP Blackholing Activity

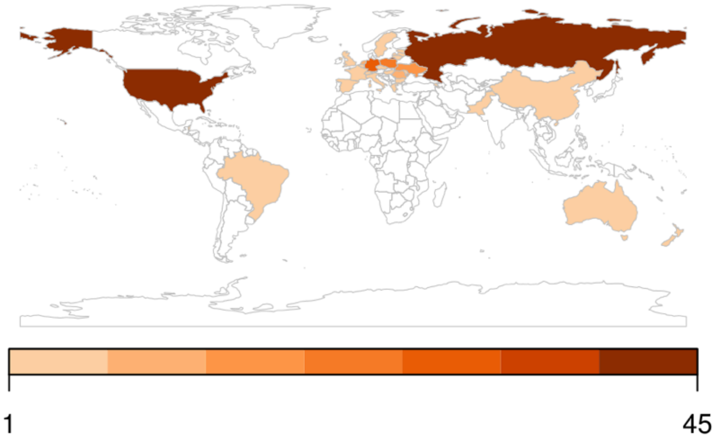
- BH providers: 100% increase, transit ASes only 18%
- BH users: 600% increase
- BH prefixes: 485 → 4,683 and 161,031 different uniques
- A) Attack on Russian gov, D) Olympic Games, E) “Kerbs on Security”

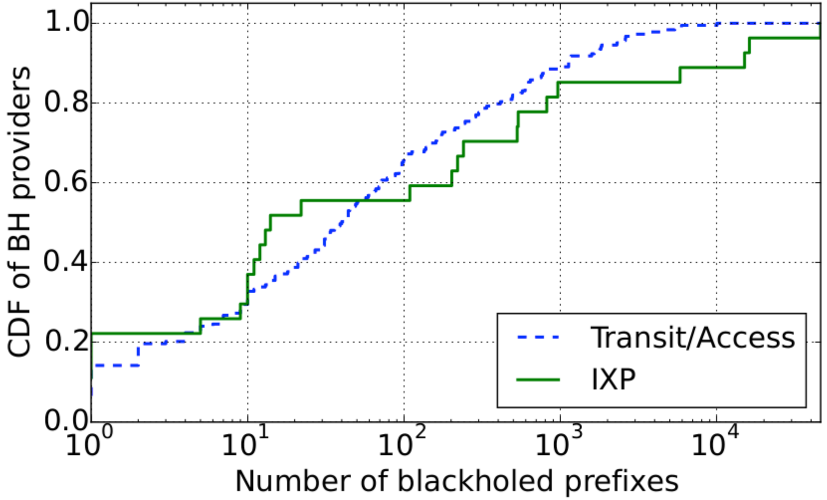






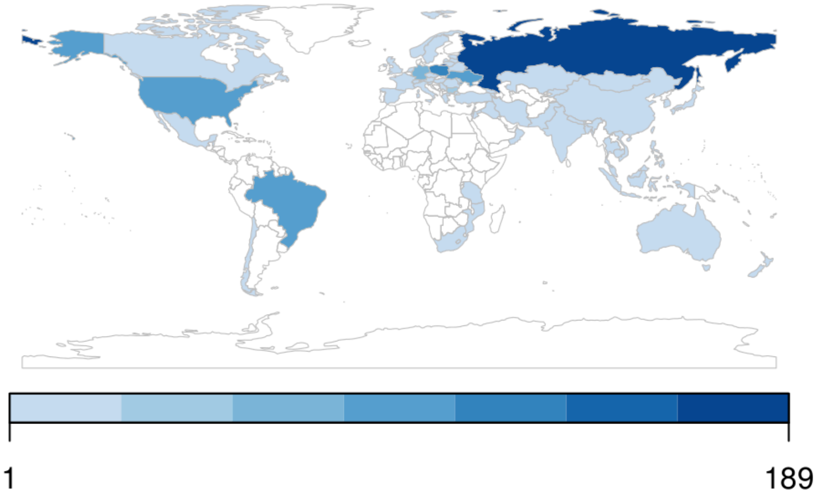
Blackholing Provider ASes

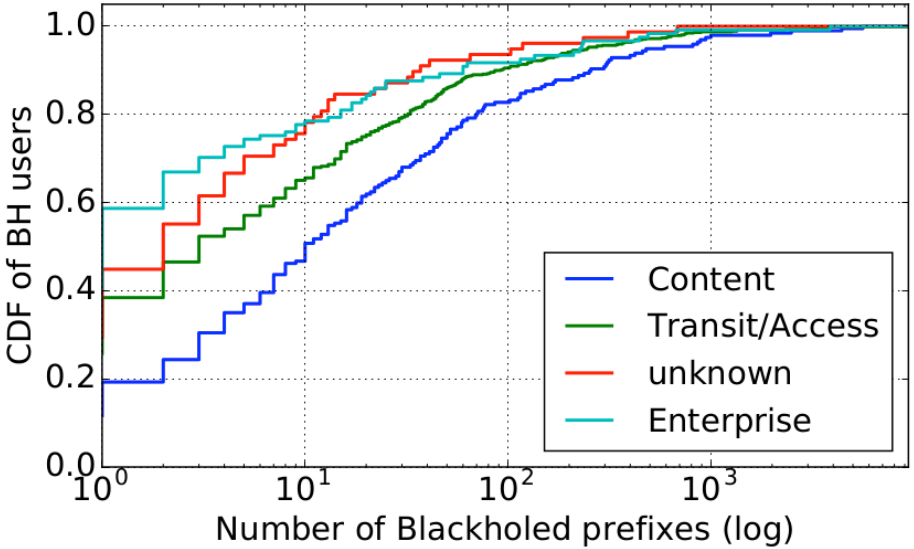




- USA, Russia, Central Europe-centric
- 184 ASes out of 242 are transit/access providers, ~10% IXPs
- Prefixes for transit/access: a few to more than 1,000, only 20 with 1000+

Blackholing User ASes

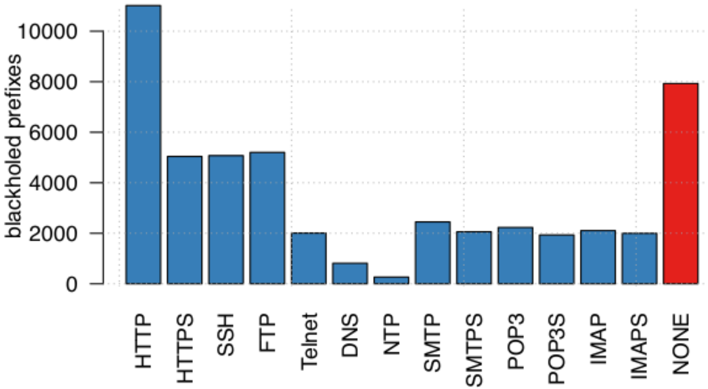




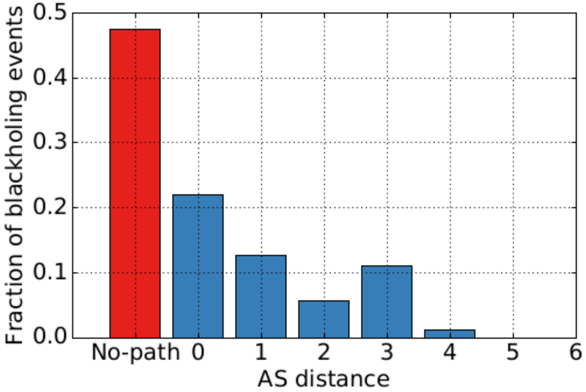
- Obviously Russia, US, and central Europe, but also Brazil and Ukraine
- Content providers dominant, 18% of users account for 43% prefixes
- Mostly small cloud providers and hosters

Blackholed Services and AS Distance

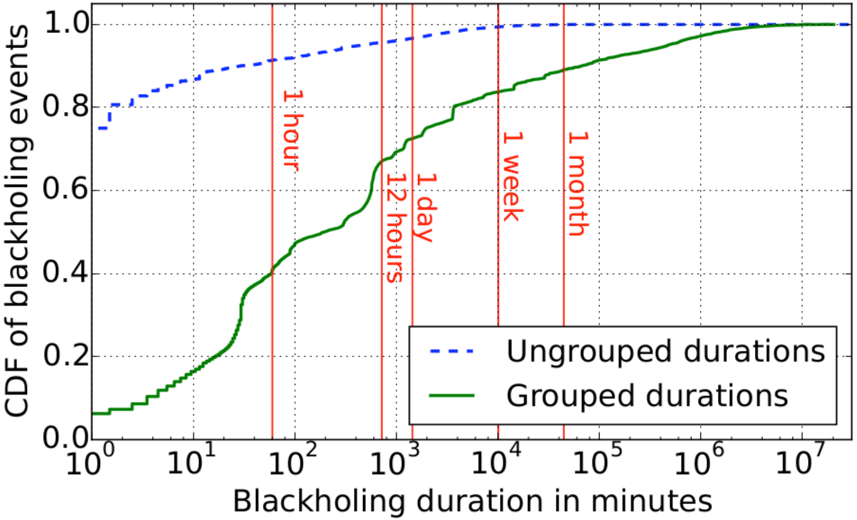
- Open host ports for 60%
  - http dominant with 53%, 61% replied to HTTP GET
  - https, ssh, ftp

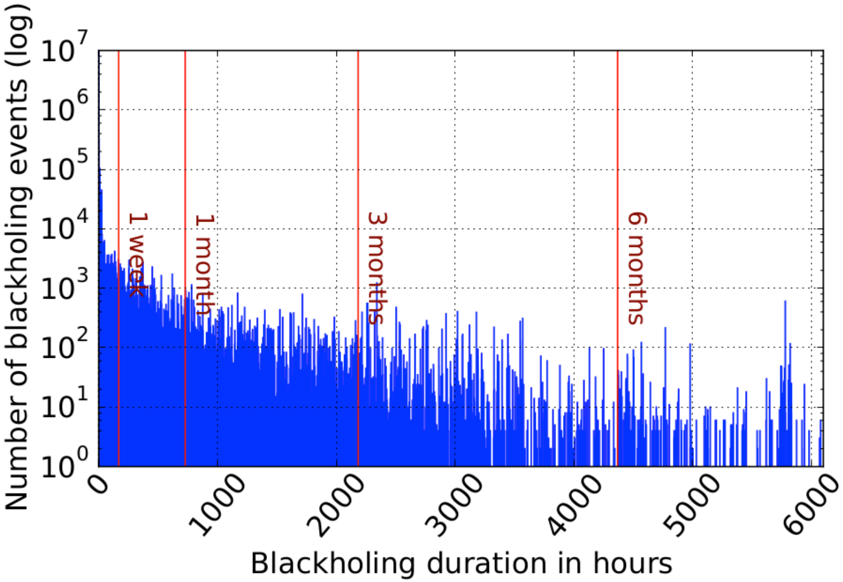


- -1: BH provider does not appear in AS path
- 0: First hop (~10%)
- 1→ 6: At least one hop (~30%)



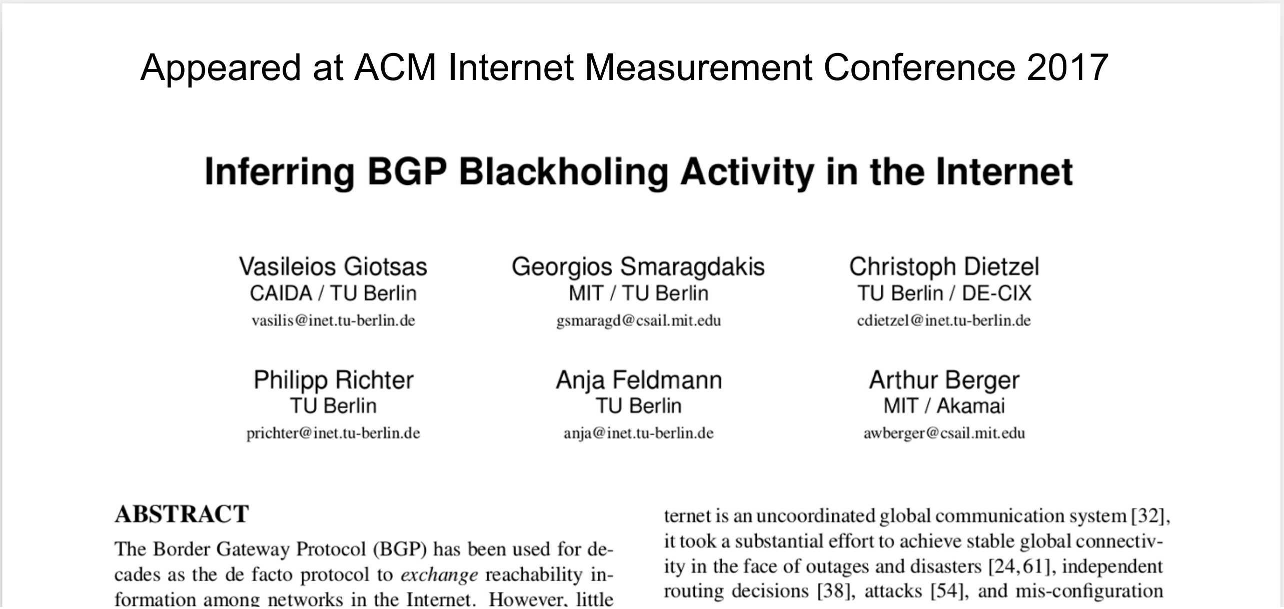
Blackholing “Events” - Durations





Conclusion

- First Internet-wide study of the state and adoption of blackholing
- Significantly increased adoption, more cyber-attacks and threats(?)
- Rise of blackholing users and prefixes, but limited geographical spread
- 400 users and up to 5K prefixes per day
- Need for more fine-grained blackholing?



Appeared at ACM Internet Measurement Conference 2017

Inferring BGP Blackholing Activity in the Internet

Vasileios Giotsas
CAIDA / TU Berlin
vasilis@inet.tu-berlin.de

Georgios Smaragdakis
MIT / TU Berlin
gsmaragd@csail.mit.edu

Christoph Dietzel
TU Berlin / DE-CIX
cdietzel@inet.tu-berlin.de

Philipp Richter
TU Berlin
prichter@inet.tu-berlin.de

Anja Feldmann
TU Berlin
anja@inet.tu-berlin.de

Arthur Berger
MIT / Akamai
awberger@csail.mit.edu

ABSTRACT

The Border Gateway Protocol (BGP) has been used for decades as the de facto protocol to *exchange* reachability information among networks in the Internet. However, little

ternet is an uncoordinated global communication system [32], it took a substantial effort to achieve stable global connectivity in the face of outages and disasters [24,61], independent routing decisions [38], attacks [54], and mis-configuration