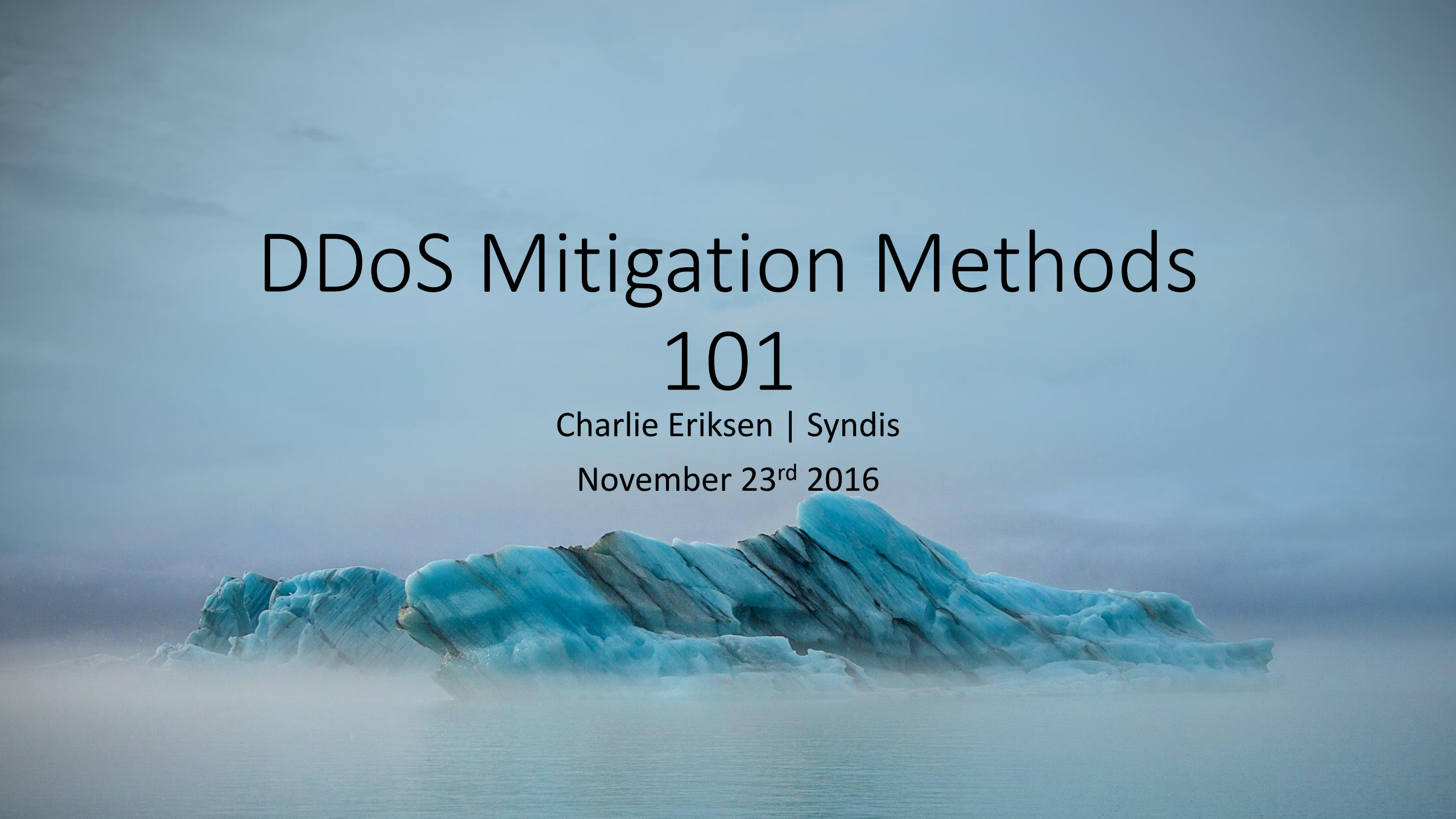


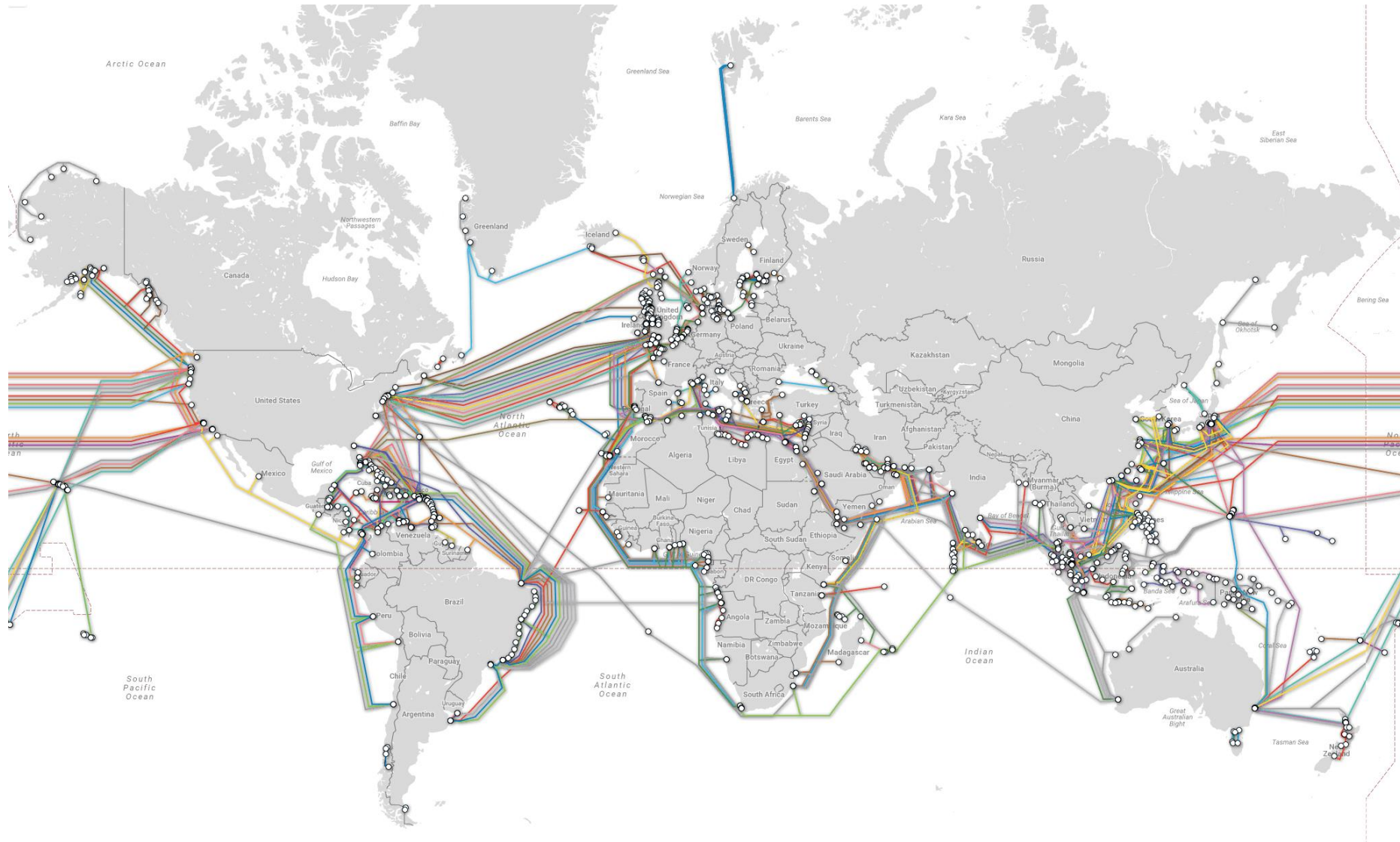
DDoS Mitigation Methods 101

Charlie Eriksen | Syndis

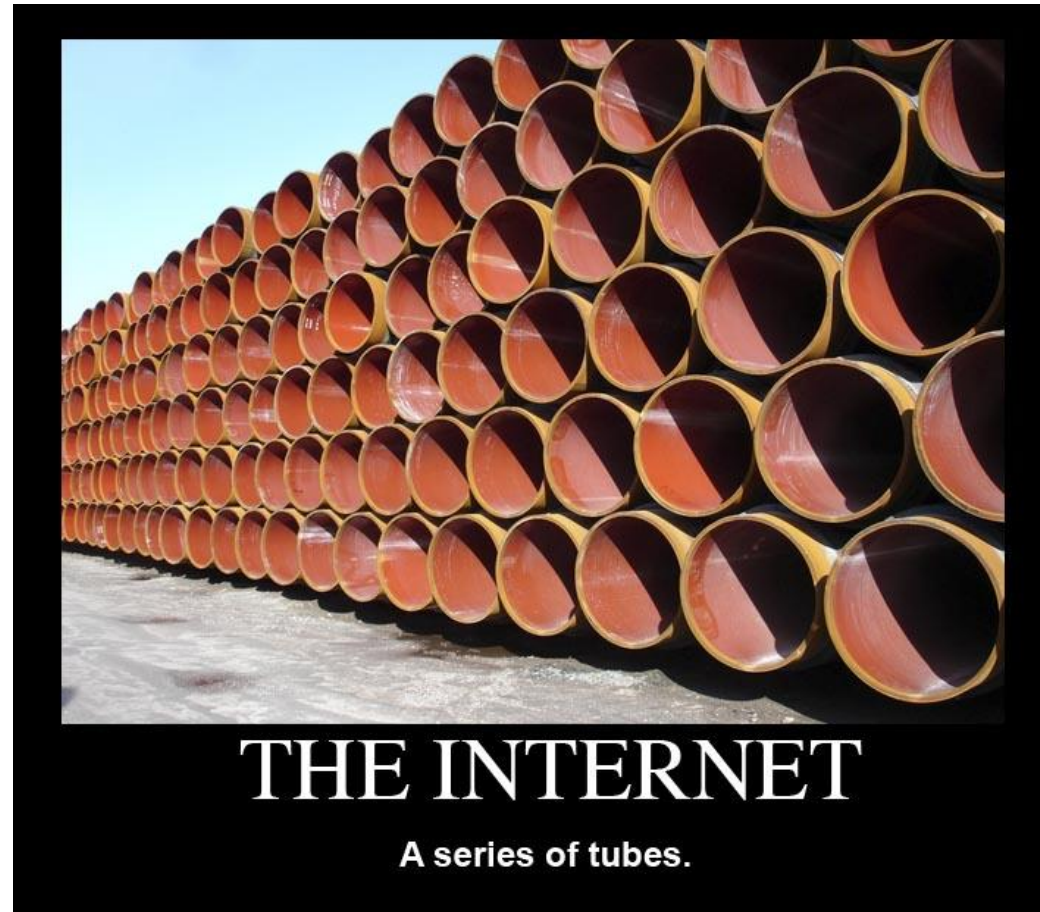
November 23rd 2016



The internet



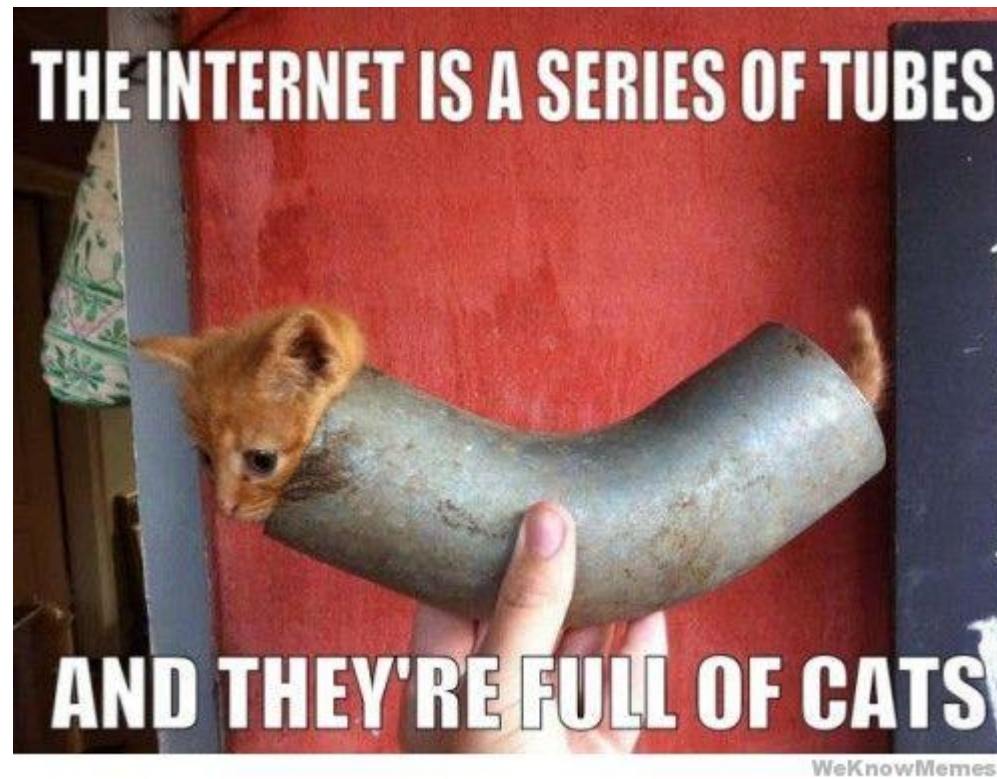
The internet



The internet



The internet



Can't you just block the IPs?

- The traffic still hits your infrastructure, so blocking the traffic won't solve the problem.

Options for mitigating too many cats

- Add more capacity/Add an in-line scrubbing box
- DNS-based reverse proxy
- BGP-based scrubbing

Adding capacity/adding in-line scrubbing box

Bigger pipes!

Protecting against what?



In-depth security news and investigation



[BLOG ADVERTISING](#) [ABOUT THE AUTHOR](#)

21 DDoS on Dyn Impacts Twitter, Spotify, Reddit

OCT 16

Criminals this morning massively attacked [Dyn](#), a company that provides core Internet services for Twitter, SoundCloud, Spotify, Reddit and a host of other sites, causing outages and slowness for many of Dyn's customers.

Home [@krebsonsec](#)

Mentions [@krebsonsec](#)

Messages (Inbox) [@krebsonsec](#)

My Tweets [@krebsonsec](#)

Twitter API is busy, please try again later

Twitter API is busy, please try again later

Twitter API is busy, please try again later

Twitter API is busy, please try again later

Twitter is experiencing problems, as seen through the social media platform Hootsuite.

In a statement, Dyn said that this morning, October 21, Dyn received a global **distributed denial of service** (DDoS) attack on its DNS infrastructure on the east coast starting at around 7:10 a.m. ET (11:10 UTC).

"DNS traffic resolved from east coast name server locations are experiencing a service interruption during this time. Updates will be posted as information becomes available," the company wrote.

DYN encouraged customers with concerns to check the company's [status page](#) for updates and to reach out to its technical support team.

A DDoS is when crooks use a large number of hacked or ill-configured systems to flood a target site with so much junk traffic that it can no longer serve legitimate visitors.

DNS refers to **Domain Name System** services. DNS is an essential component of all Web sites, responsible for translating human-friendly Web site names like "example.com" into numeric, machine-readable Internet addresses. Anytime you send an e-mail or browse a Web site, your machine is sending a DNS look-up request to your Internet service provider to help route the traffic.

SPAM NATION

NEW YORK TIMES BESTSELLER



THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR

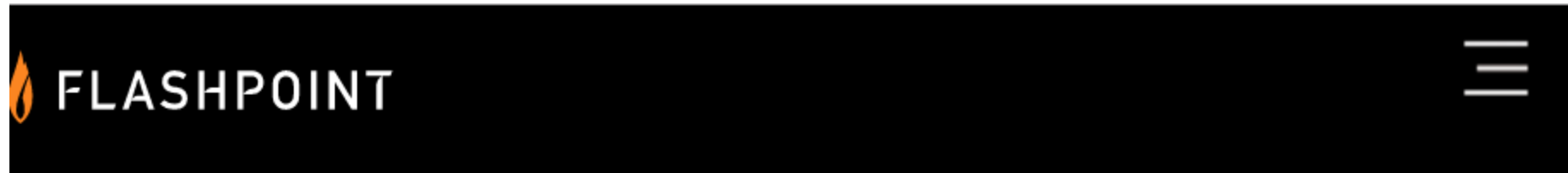
BRIAN KREBS

FOREWORD BY THE ARCADE FIRE • INTRODUCED BY TONY HILL • ILLUSTRATIONS BY TONY HILL

A New York Times Bestseller!

Buy at Amazon











Magnitude



Flashpoint assesses with moderate confidence that the Command and Control server used in the Dyn DNS attack was separate and distinct from those used in the Krebs and OVH attacks. It is unknown how the most recent attack compares to previous ones, and the size and scale of the infrastructure used. The previous Mirai attacks against OVH and Krebs were recorded at approximately 1 Tbps and 620 Gbps, respectively.

Magnitude

Akamai Q4 2015 global average connection speeds rankings

Rank ↕	Country/Territory ↕	Avg. connection speed (Mb/s) ^[2] ↕	Relative speed ↕
-	Global	5.6	<div></div>
1	 South Korea	26.7	<div></div>
2	 Sweden	19.1	<div></div>
3	 Norway	18.8	<div></div>
4	 Japan	17.4	<div></div>
5	 Netherlands	17.0	<div></div>
6	 Hong Kong	16.8	<div></div>
7	 Latvia	16.7	<div></div>
8	 Switzerland	16.7	<div></div>
9	 Finland	16.6	<div></div>
10	 Denmark	16.1	<div></div>

Magnitude

Type	Speed
Average Danish internet speed	16.1 Mbit/s
Normal consumer local network	100 Mbit/s
Icelandic min. fiber speed	100 Mbit/s
Icelandic top fiber speed	500 Mbit/s – 1 Gbit/s
Normal hosting speed	1 – 10 Gbit/s
Average DDoS attack speed	6.88 Gbit/s
Biggest DDoS attacks known	630 – 1.000 Gbit/s

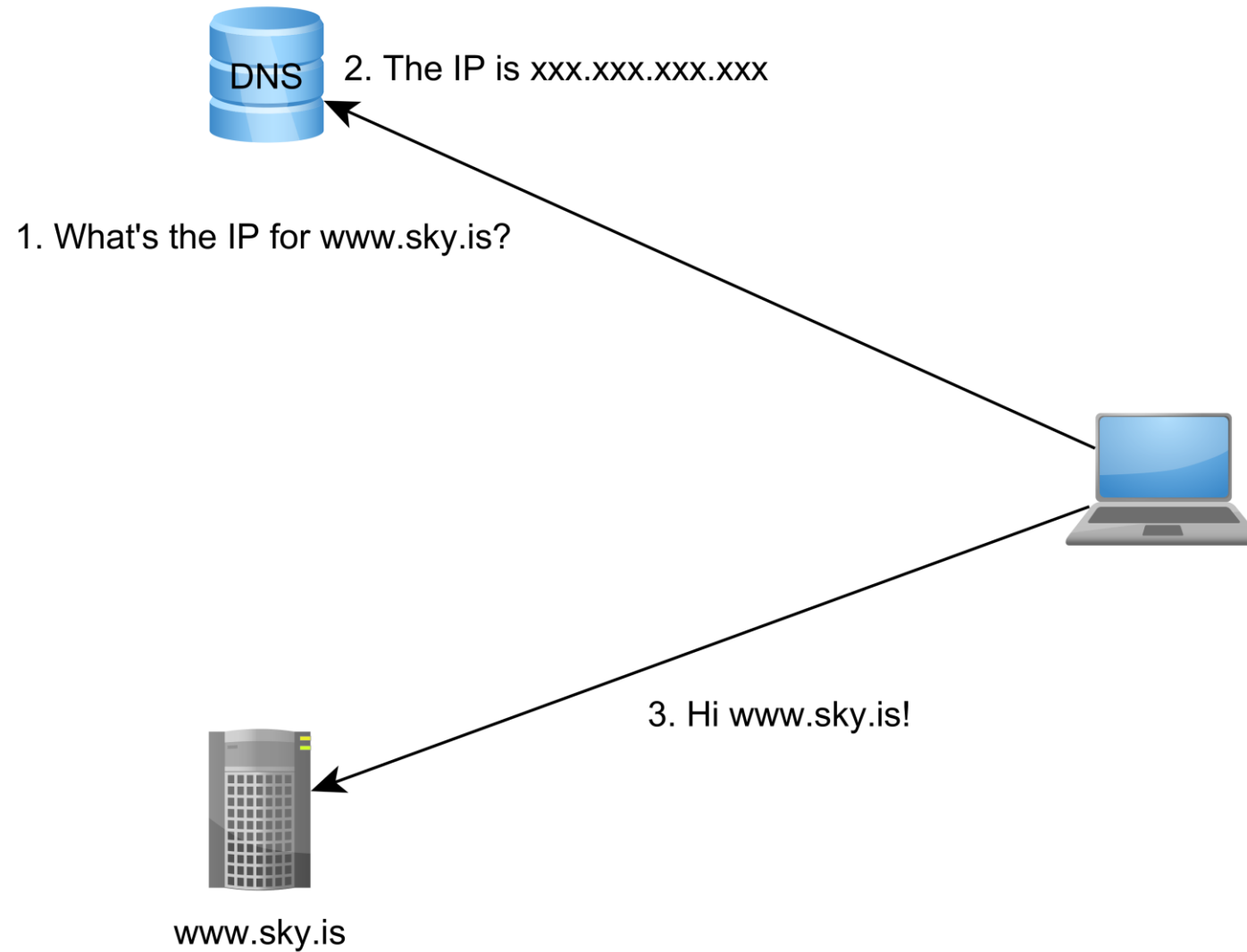
Adding more capacity

- If you are not an ISP, this probably won't help.
- You'd need to wire everything at least 10gbit, and hope you won't hit CPU caps.
- You can add a scrubbing-box, if you have the capacity

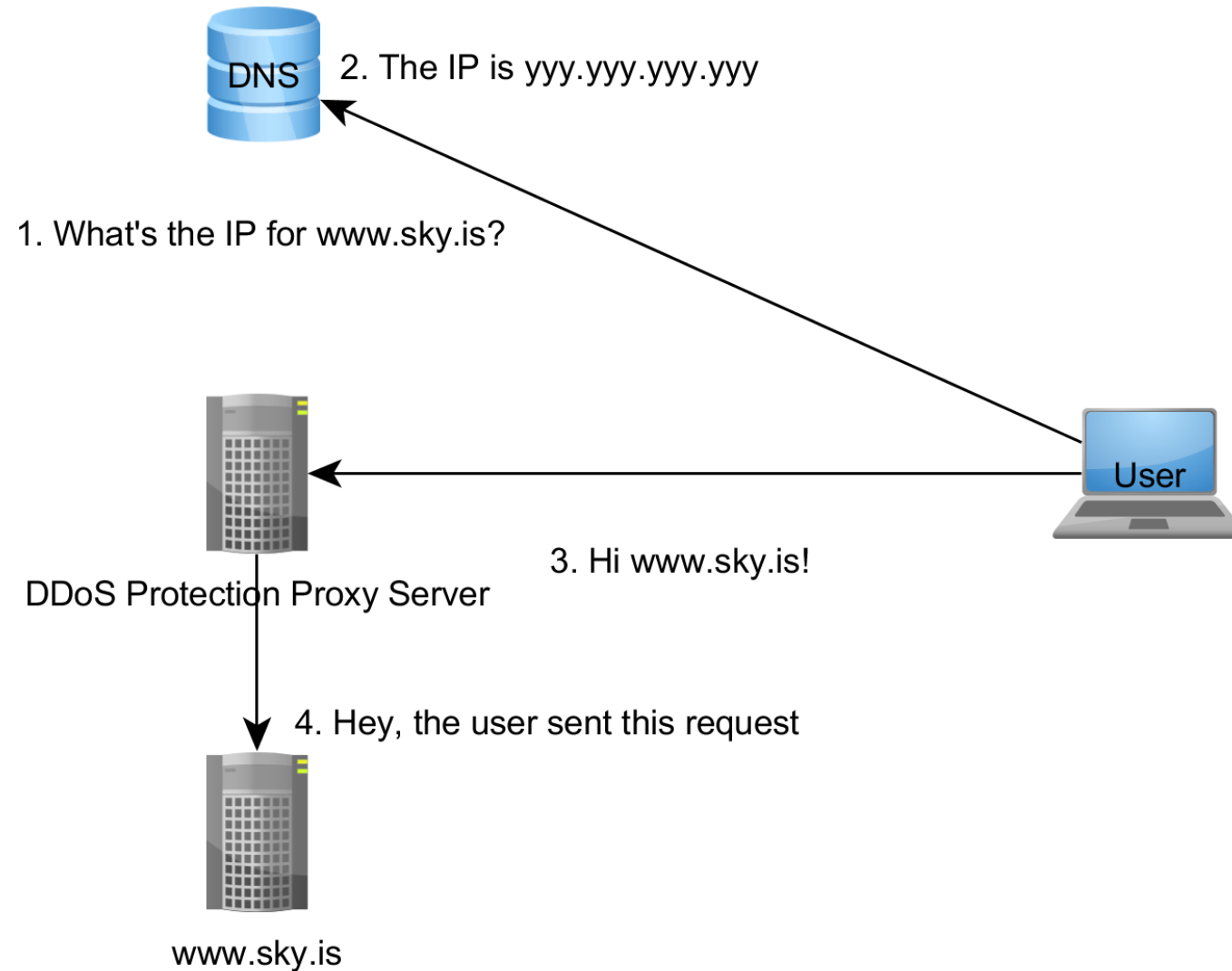
DNS Proxy Service

HTTP-Only protection!

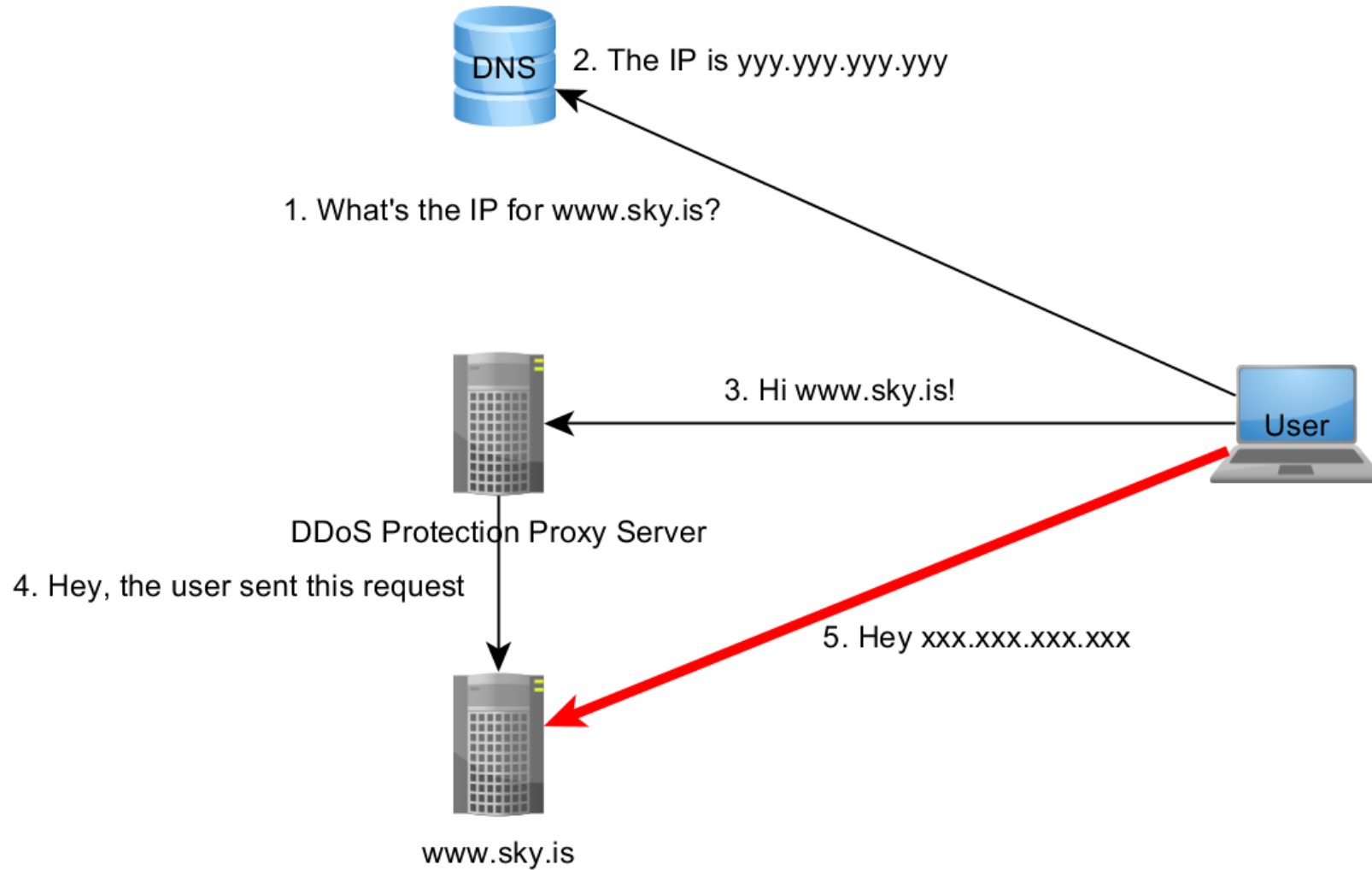
DNS 101



DNS Proxy Service



Pitfall



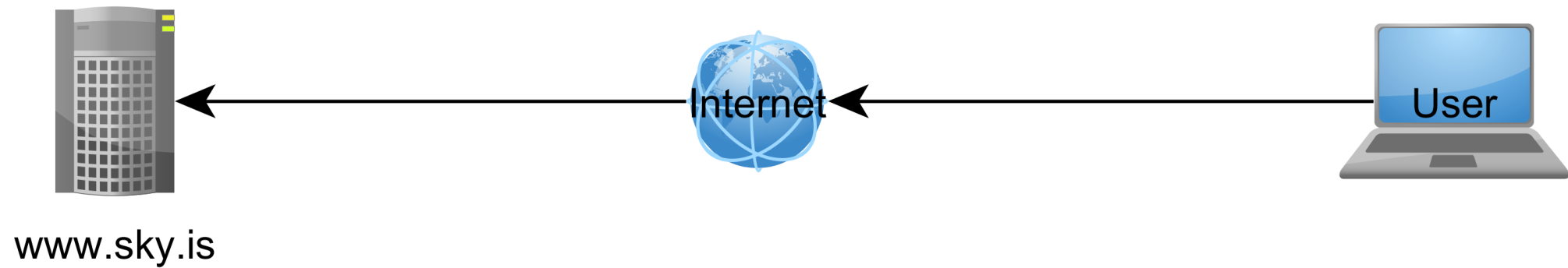
Summary

- Pros
 - Relatively cheap
 - Has a lot of value-adds
 - If you don't have a complex infrastructure, it is easy to use
 - Proactive
- Cons
 - Requires you to move your DNS
 - If you have fixed IPs in a single location, you aren't protected
 - Can be misconfigured
 - All your data goes through a third-party abroad

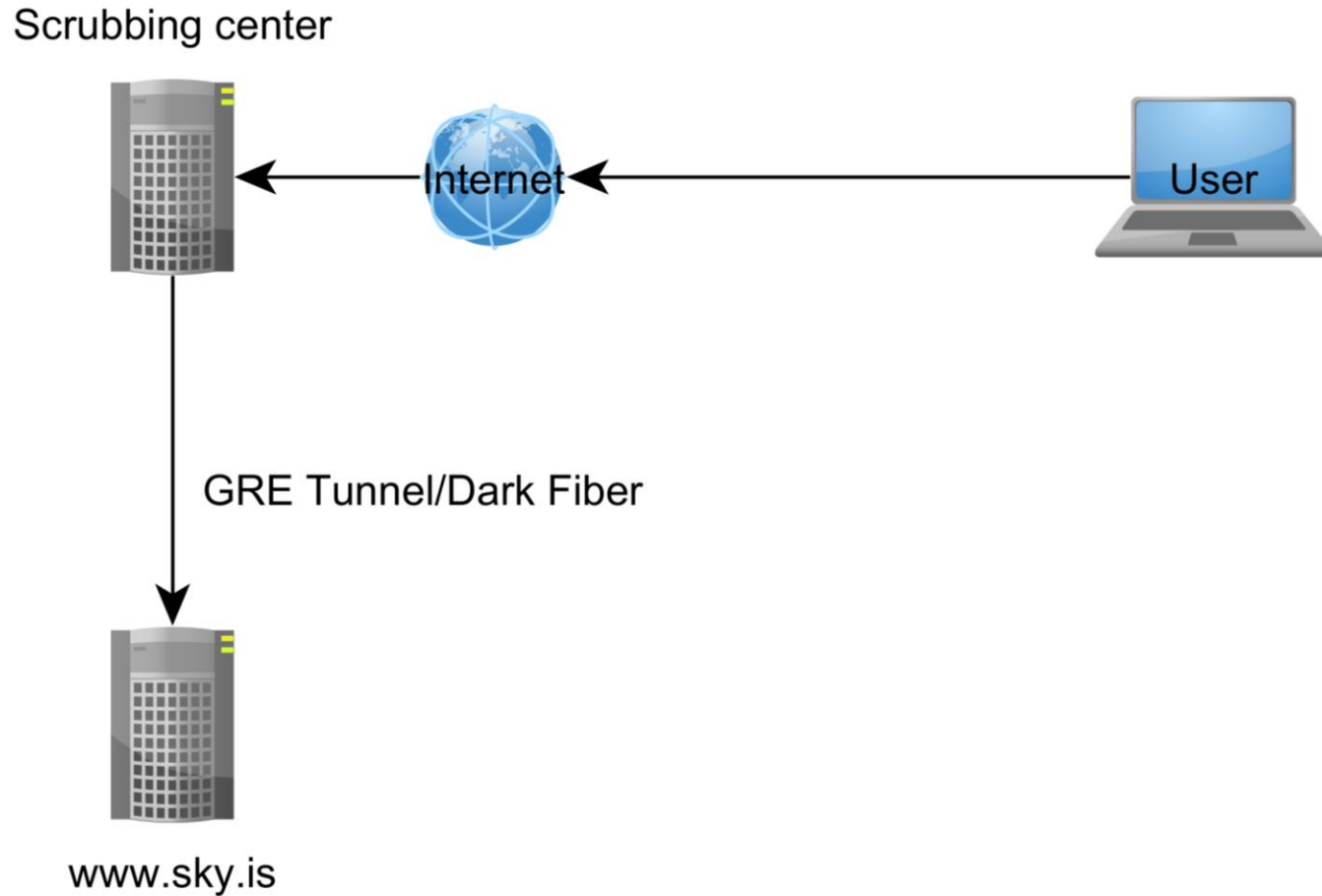
BGP Scrubbing Services

Rewire the pipes!

BGP Scrubbing Services



BGP Scrubbing Services



Requirements

- Will usually need an ASN, and a IP allocation (For true in-line)
- Need to set up a GRE, and/or dark fiber
- Hybrid solutions exist
 - You'll get assigned an IP from the vendor
 - If you are tunneling back to your site, issues can still happen

What happens?

1. When you are under attack, you need to engage the BGP swing*
2. You stop advertising your ASN, and the mitigation company starts advertising it instead
3. They start receiving the traffic, and route it to you over the GRE


* Unless you have an always-on service (\$\$\$\$)

Pros/cons


- Pros
 - For complex infrastructure, it's the only good solution
- Cons
 - Expensive
 - All your traffic is routed through, and inspected by a third party
 - More complex setup
 - Custom protocols can be problematic

Cons

Krebs on Security
In-depth security news and investigation




[BLOG ADVERTISING](#) [ABOUT THE AUTHOR](#)



11 Hackers Target Anti-DDoS Firm Staminus

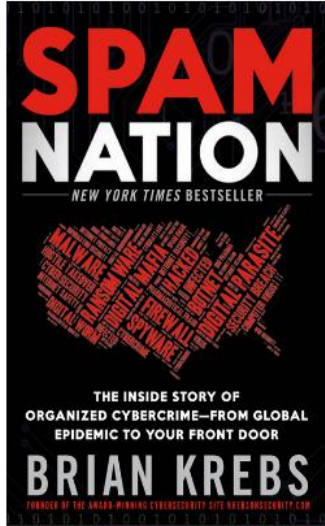
MAR 16

Staminus Communications Inc., a California-based Internet hosting provider that specializes in protecting customers from massive “distributed denial of service” (DDoS) attacks aimed at knocking sites offline, has itself apparently been massively hacked. Staminus’s entire network was down for more than 20 hours until Thursday evening, leaving customers to vent their rage on the company’s Facebook and Twitter pages. In the midst of the outage, someone posted online download links for what appear to be Staminus’s customer credentials, support tickets, credit card numbers and other sensitive data.





The e-zine posted online Thursday following an outage at Staminus Communications.

My New Book!



A New York Times Bestseller!

[Buy at Amazon](#) 

[Donate with PayPal](#) 

Recent Posts

- [Adobe Fined \\$1M in Multistate Suit Over 2013 Breach; No Jail for Spamhaus Attacker](#)
- [Chinese IoT Firm Siphoned Text](#)

Summary

