Digital Attack Map

http://www.digitalattackmap.com/

Top daily DDoS attacks worldwide

What does Digital Attack Map perform?

- Live Visualization of DDoS attacks around the globe.
- Google Ideas + Big Picture + Arbor

Google Ideas : Protecting the people from online harassment. (Build new technology to mitigate the threats)

Big Picture : They blend algorithmic, data-driven approaches with fluid design to make complex data more accessible.

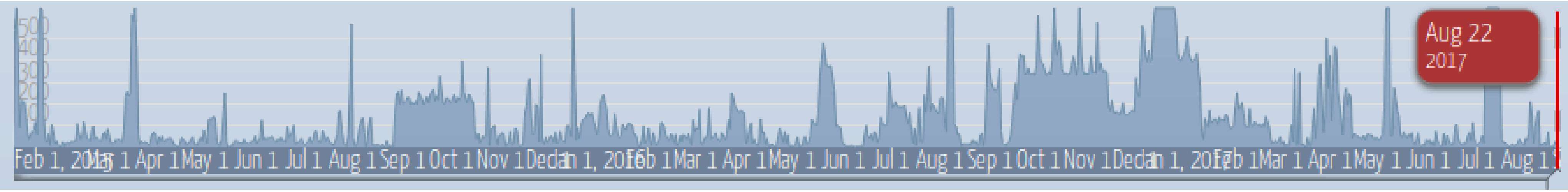
ARBOR : Provide DDoS attack data.

What is a DDoS attack ?

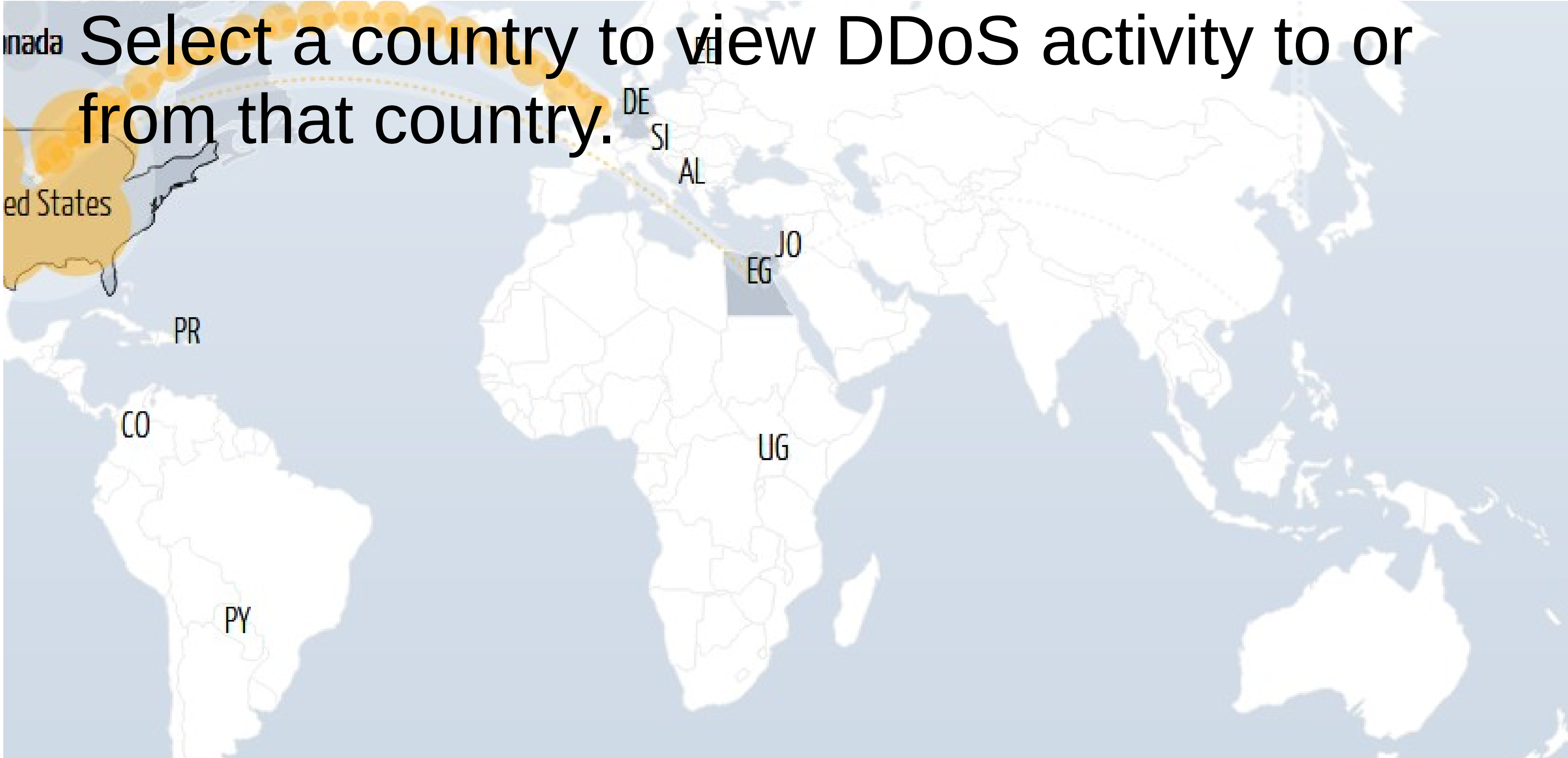
- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.

Exploring Data

Use the histogram at the bottom of the map to explore historical data.



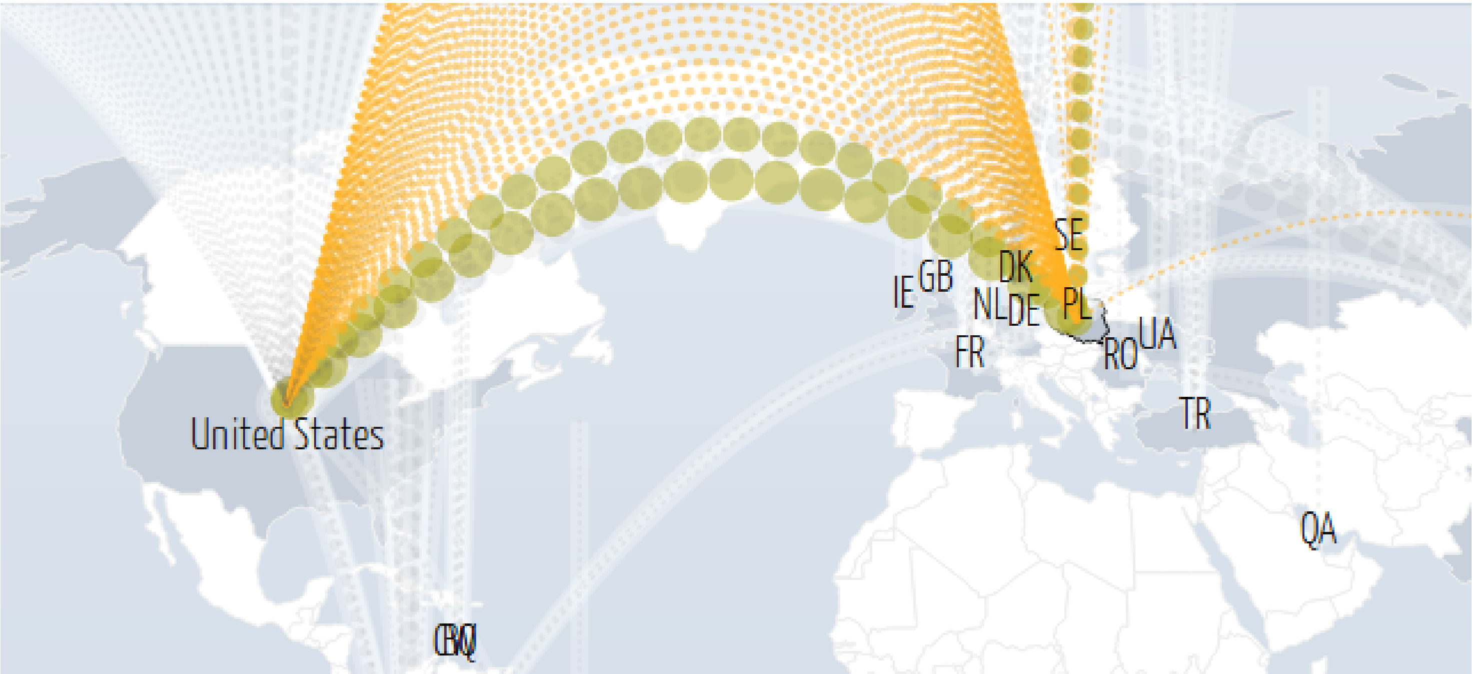
Exploring Data



Select a country to view DDoS activity to or from that country.

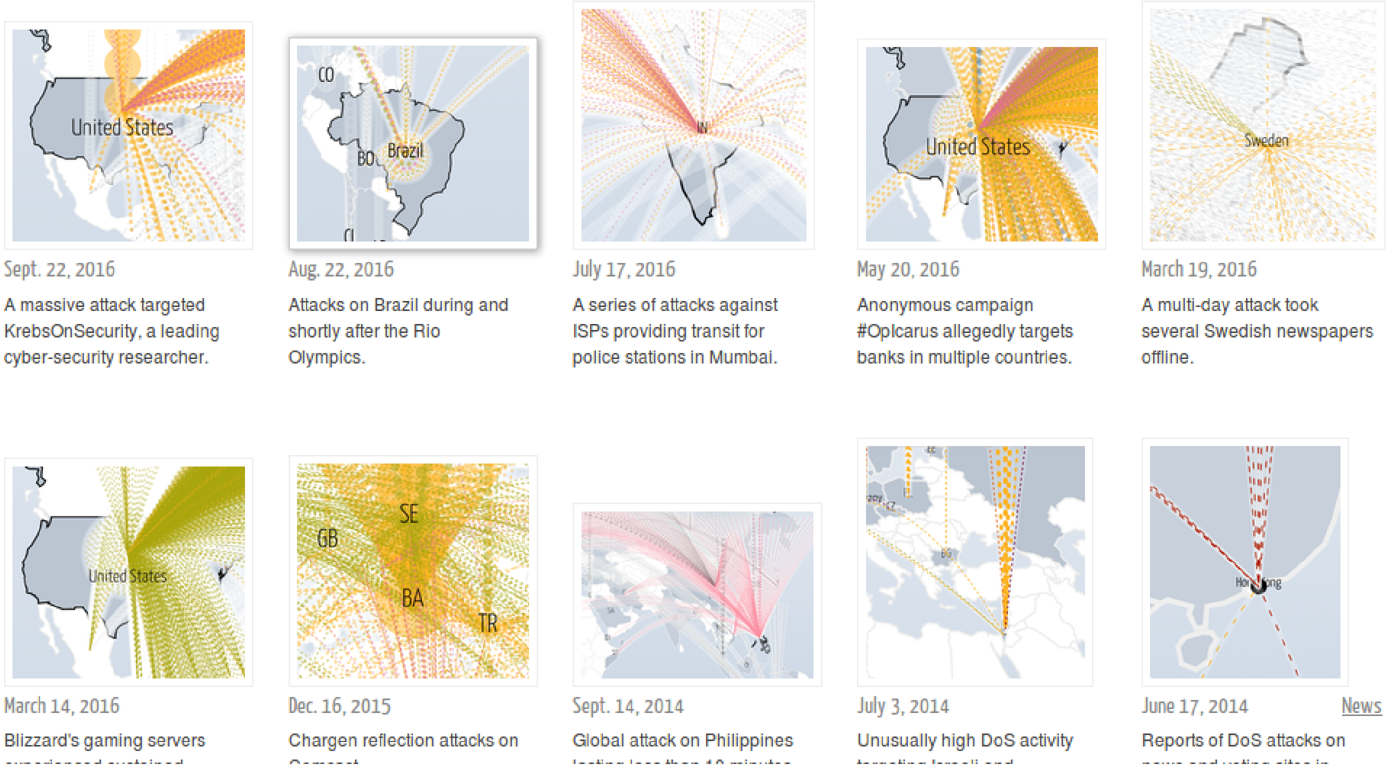
Exploring Data

Use the color option to view attacks by class, duration, or source/destination port.



Exploring Data

Use the news section to find online reports of attack activity from a specified time.



Sept. 22, 2016
A massive attack targeted KrebsOnSecurity, a leading cyber-security researcher.

Aug. 22, 2016
Attacks on Brazil during and shortly after the Rio Olympics.

July 17, 2016
A series of attacks against ISPs providing transit for police stations in Mumbai.

May 20, 2016
Anonymous campaign #OpIcarus allegedly targets banks in multiple countries.

March 19, 2016
A multi-day attack took several Swedish newspapers offline.

March 14, 2016
Blizzard's gaming servers

Dec. 16, 2015
Chargen reflection attacks on

Sept. 14, 2014
Global attack on Philippines

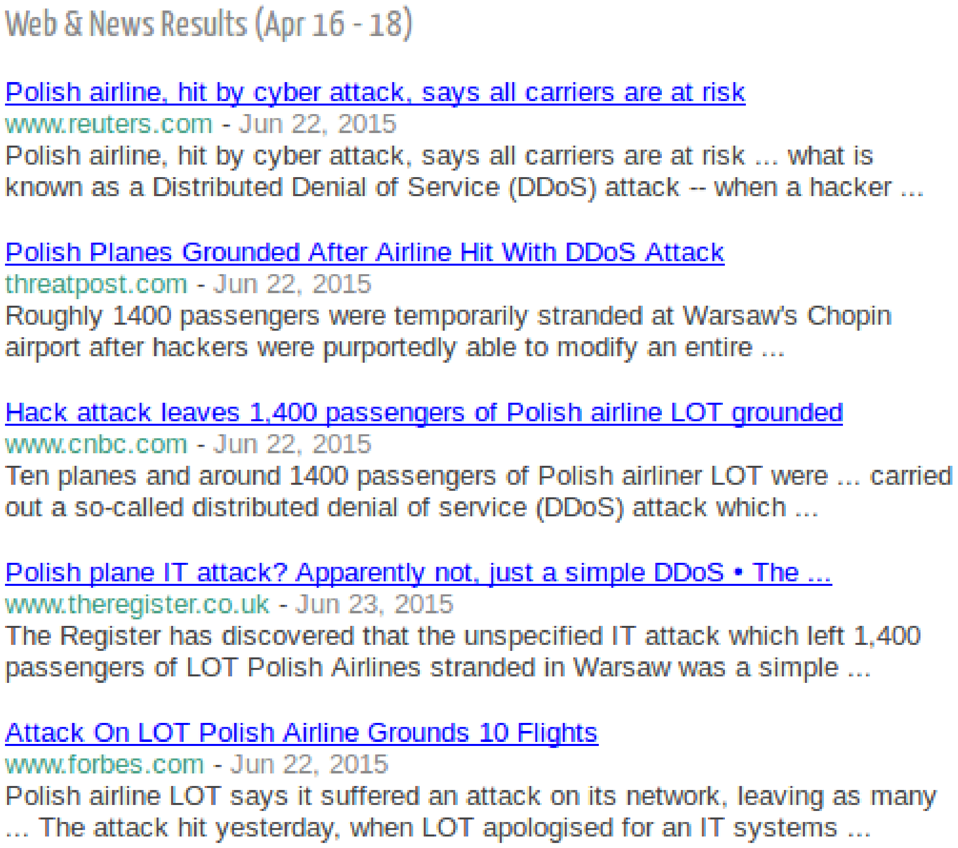
July 3, 2014
Unusually high DoS activity

June 17, 2014
Reports of DoS attacks on

News

Exploring Data

View the gallery to explore some examples of days with notable DDoS attacks.



Web & News Results (Apr 16 - 18)

Polish airline, hit by cyber attack, says all carriers are at risk
www.reuters.com - Jun 22, 2015
Polish airline, hit by cyber attack, says all carriers are at risk ... what is known as a Distributed Denial of Service (DDoS) attack -- when a hacker ...

Polish Planes Grounded After Airline Hit With DDoS Attack
threatpost.com - Jun 22, 2015
Roughly 1400 passengers were temporarily stranded at Warsaw's Chopin airport after hackers were purportedly able to modify an entire ...

Hack attack leaves 1,400 passengers of Polish airline LOT grounded
www.cnbc.com - Jun 22, 2015
Ten planes and around 1400 passengers of Polish airliner LOT were ... carried out a so-called distributed denial of service (DDoS) attack which ...

Polish plane IT attack? Apparently not, just a simple DDoS • The ...
www.theregister.co.uk - Jun 23, 2015
The Register has discovered that the unspecified IT attack which left 1,400 passengers of LOT Polish Airlines stranded in Warsaw was a simple ...

Attack On LOT Polish Airline Grounds 10 Flights
www.forbes.com - Jun 22, 2015
Polish airline LOT says it suffered an attack on its network, leaving as many ... The attack hit yesterday, when LOT apologised for an IT systems ...

Examples of DDoS attacks

- Smurfs

  Large number of ICMP message can slow down the victims computer/server.

- Teardrops

  Sending oversized payloads to the target machine to crash.

- Ping of Death

  Make the buffer to overflow which can crash the system.

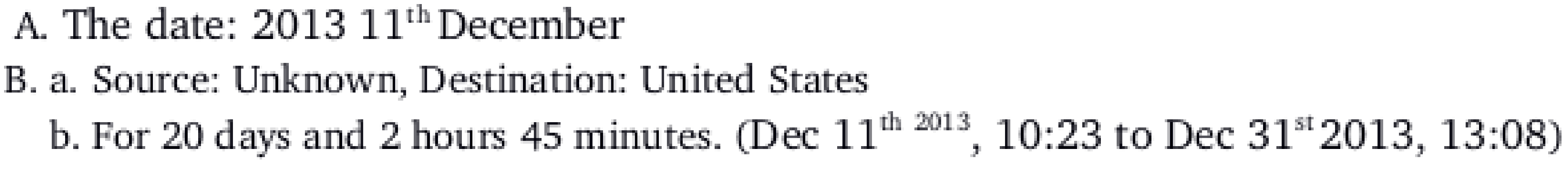
Types of Attacks in Digital Map

- TCP Connection Attack
- Volumetric Attack
- Fragmentation Attack
- Application Attack

TCP Connection Attack

These attempt to use up all the available connections to infrastructure devices such as load-balancers, firewalls and application servers. Even devices capable of maintaining state on millions of connections can be taken down by these attacks.

E.g.



A. The date: 2013 11th December

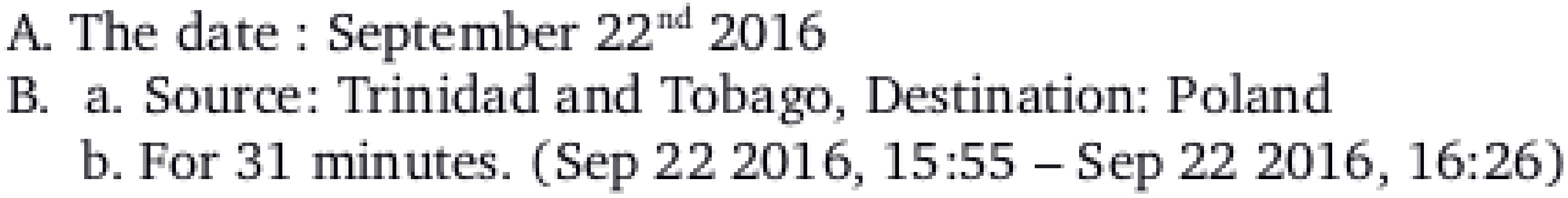
B. a. Source: Unknown, Destination: United States

b. For 20 days and 2 hours 45 minutes. (Dec 11th 2013, 10:23 to Dec 31st 2013, 13:08)

Volumetric Attack

These attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.

E.g.



A. The date : September 22nd 2016

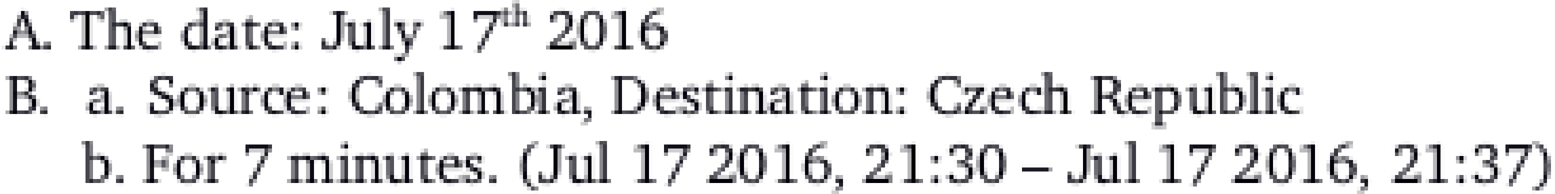
B. a. Source: Trinidad and Tobago, Destination: Poland

   b. For 31 minutes. (Sep 22 2016, 15:55 – Sep 22 2016, 16:26)

Fragmentation Attack

These send a flood of TCP or UDP fragments to a victim, overwhelming the victim's ability to re-assemble the streams and severely reducing performance

E.g.



A. The date: July 17th 2016

B. a. Source: Colombia, Destination: Czech Republic

b. For 7 minutes. (Jul 17 2016, 21:30 – Jul 17 2016, 21:37)

Application Attack

These attempt to overwhelm a specific aspect of an application or service and can be effective even with very few attacking machines generating a low traffic rate (making them difficult to detect and mitigate).

1. DNS Reflection - Small request, big reply

2. Chargen Reflection - Steady streams of text