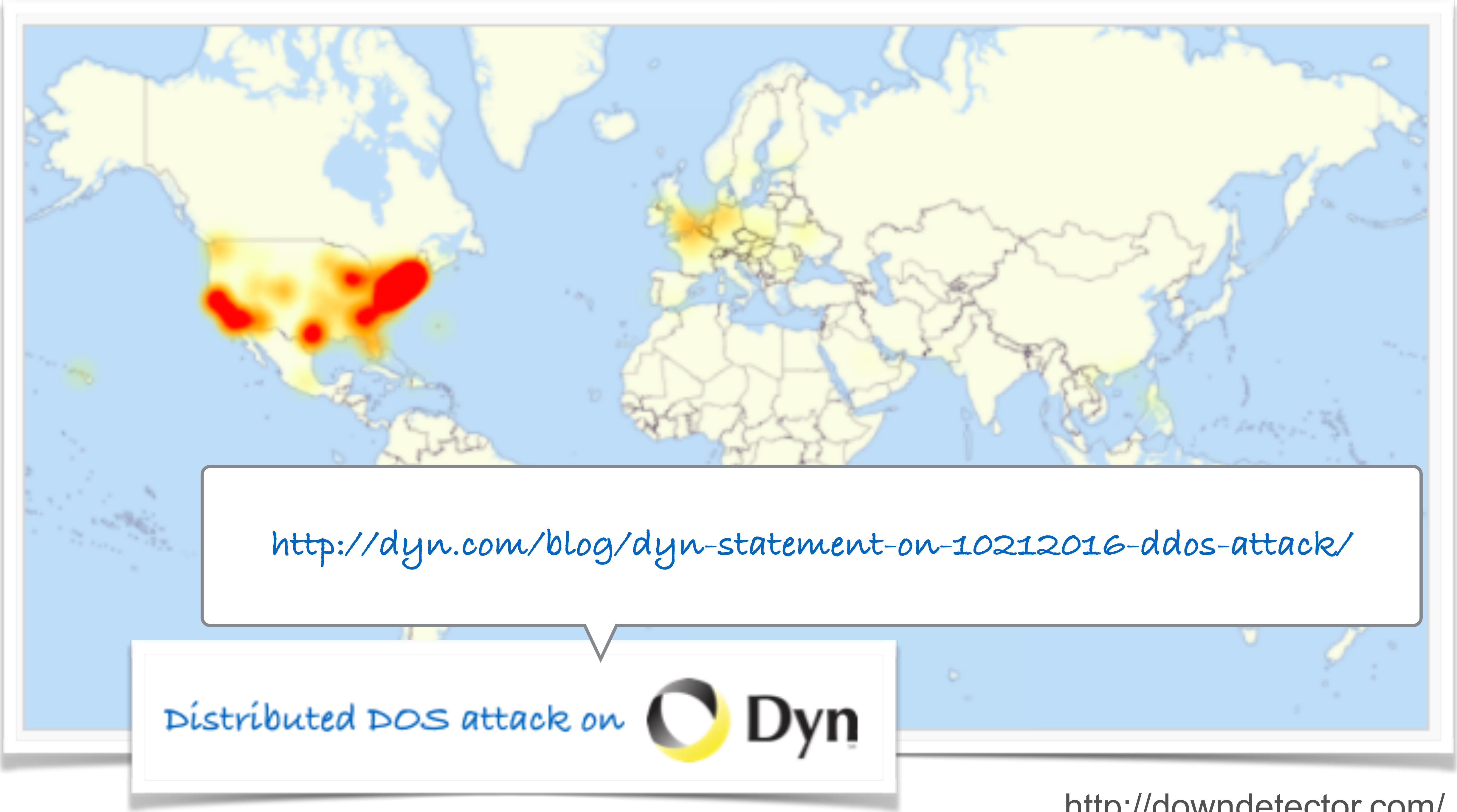
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

DDos Prevention and Mitigation

Christian Teuschel | November 2016 | Skopje

Friday, 21 October 2016



http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Distributed DOS attack on Dyn

http://downdetector.com/

Denial-Of-Service 101

- What?
  - Attack on IT infrastructure
  - Make machine/network resource unavailable
  - Temporary or indefinite

  - Not a new invention!

Denial-Of-Service 101

- How?
  - Crashing service
  - Flooding service
- Effect
  - Prevent legitimate users to be serviced

Denial-Of-Service 101

- Targets:
  - Usually high-profile sites
  - But not only
- Initiators
  - Hackers
  - Script kids
  - Criminals
  - State actor
  - Insider

Denial-Of-Service 101

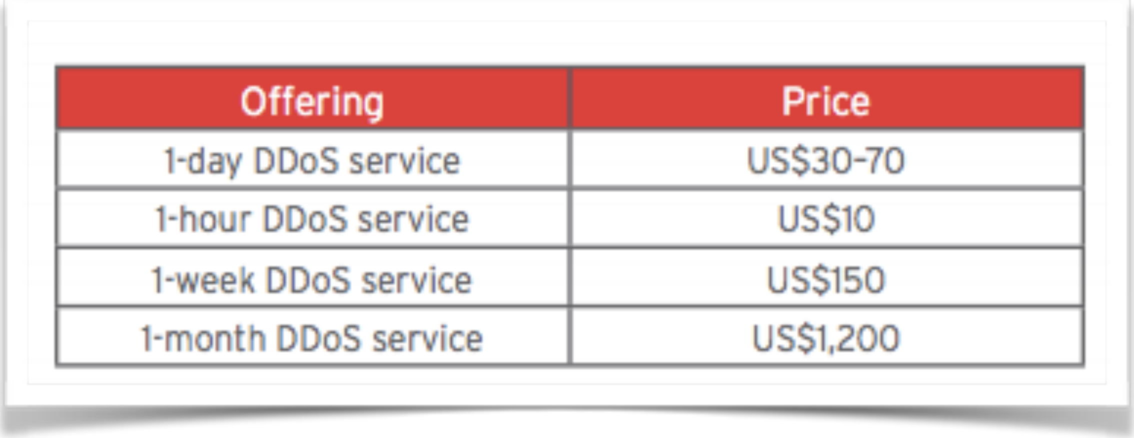
- Costs
  - Mitigation costs
  - Lost revenue
  - Reputation

Special Forms Of DOS

- Distributed DOS
  - Involving multiple devices in the attack

Focus

- APDOS
  - Involving an advanced persistent thread
  - Requires resources and sophistication
- DOS as a service
  - Entry barrier is getting lower
  - Growing market



Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

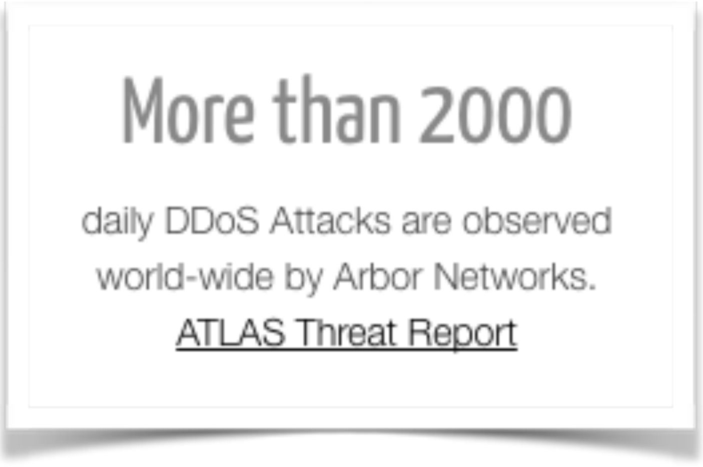
DDoS Attack Classes

- TCP Connection Attack
  - Intention to use up available connections
- Volumetric Attack
  - Intention to cause congestions
- Fragmentation Attack
  - Intention to overwhelm request handling
- Application Attack
  - Intention to exploit specific aspects of an application

DDoS Amplification

- DNS Reflection
  - Small request, big response
- Chargen Reflection
  - Streams of random characters on demand

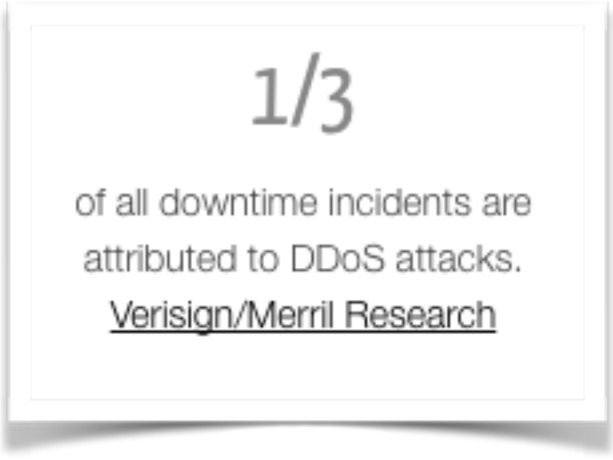
Statistics on DDos



More than 2000

daily DDoS Attacks are observed world-wide by Arbor Networks.

ATLAS Threat Report

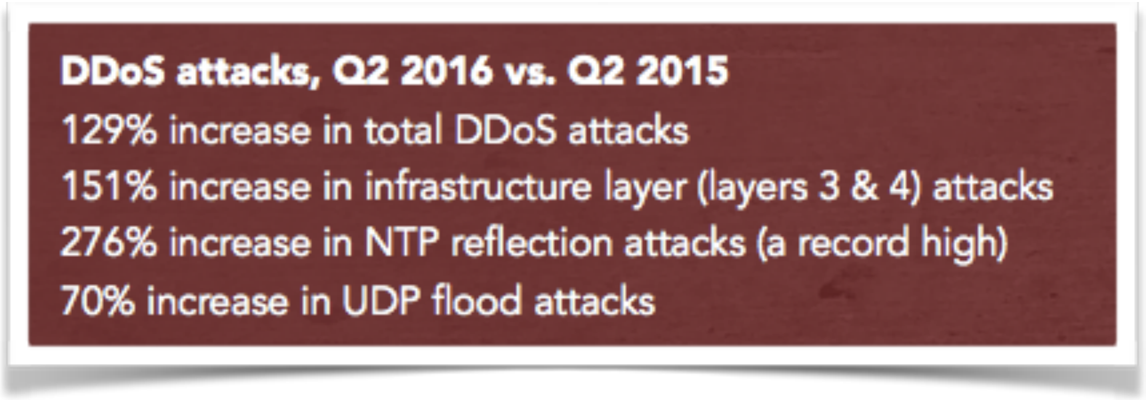


1/3

of all downtime incidents are attributed to DDoS attacks.

Verisign/Merril Research

http://www.digitalattackmap.com/



DDoS attacks, Q2 2016 vs. Q2 2015

129% increase in total DDoS attacks

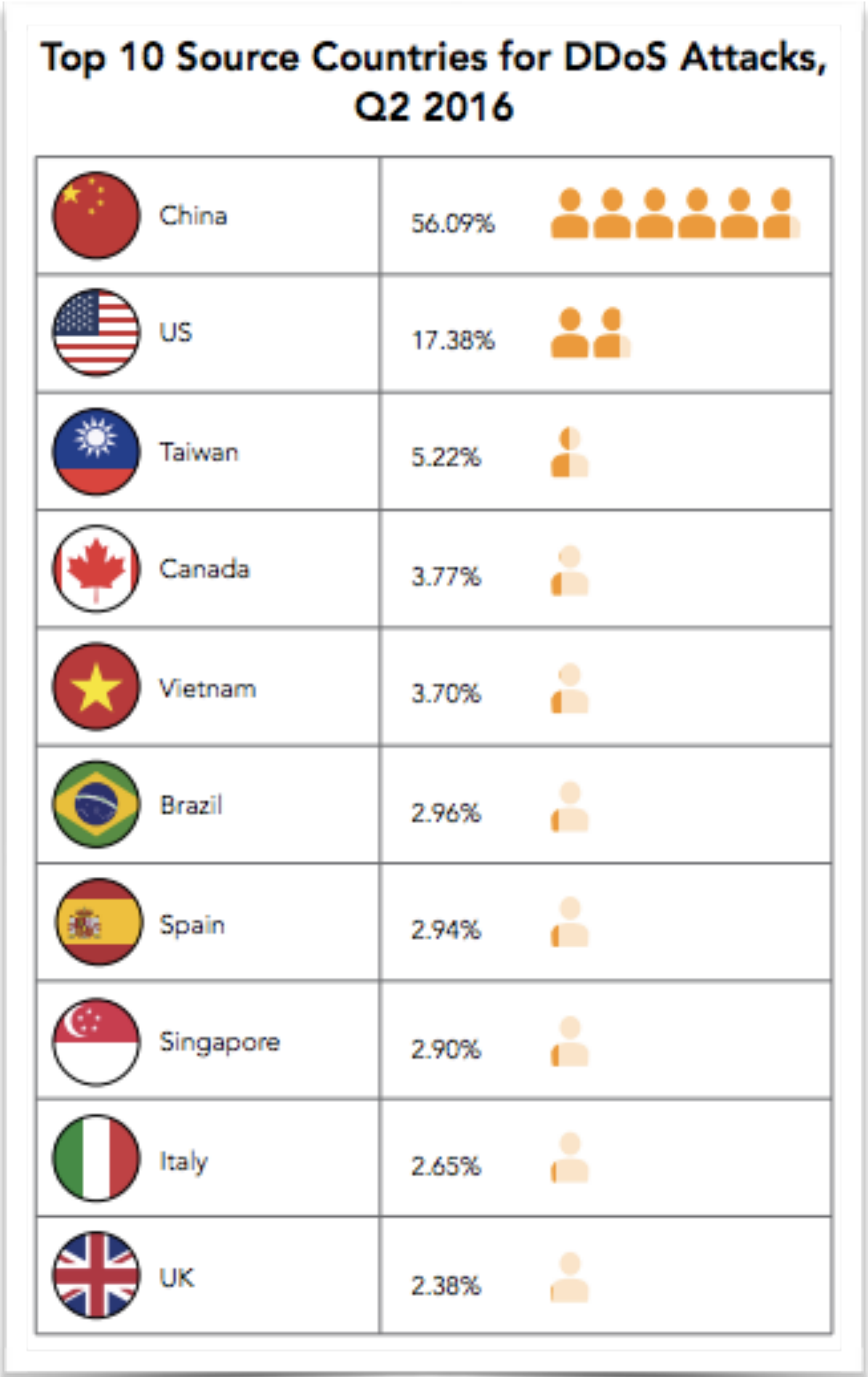
151% increase in infrastructure layer (layers 3 & 4) attacks

276% increase in NTP reflection attacks (a record high)

70% increase in UDP flood attacks

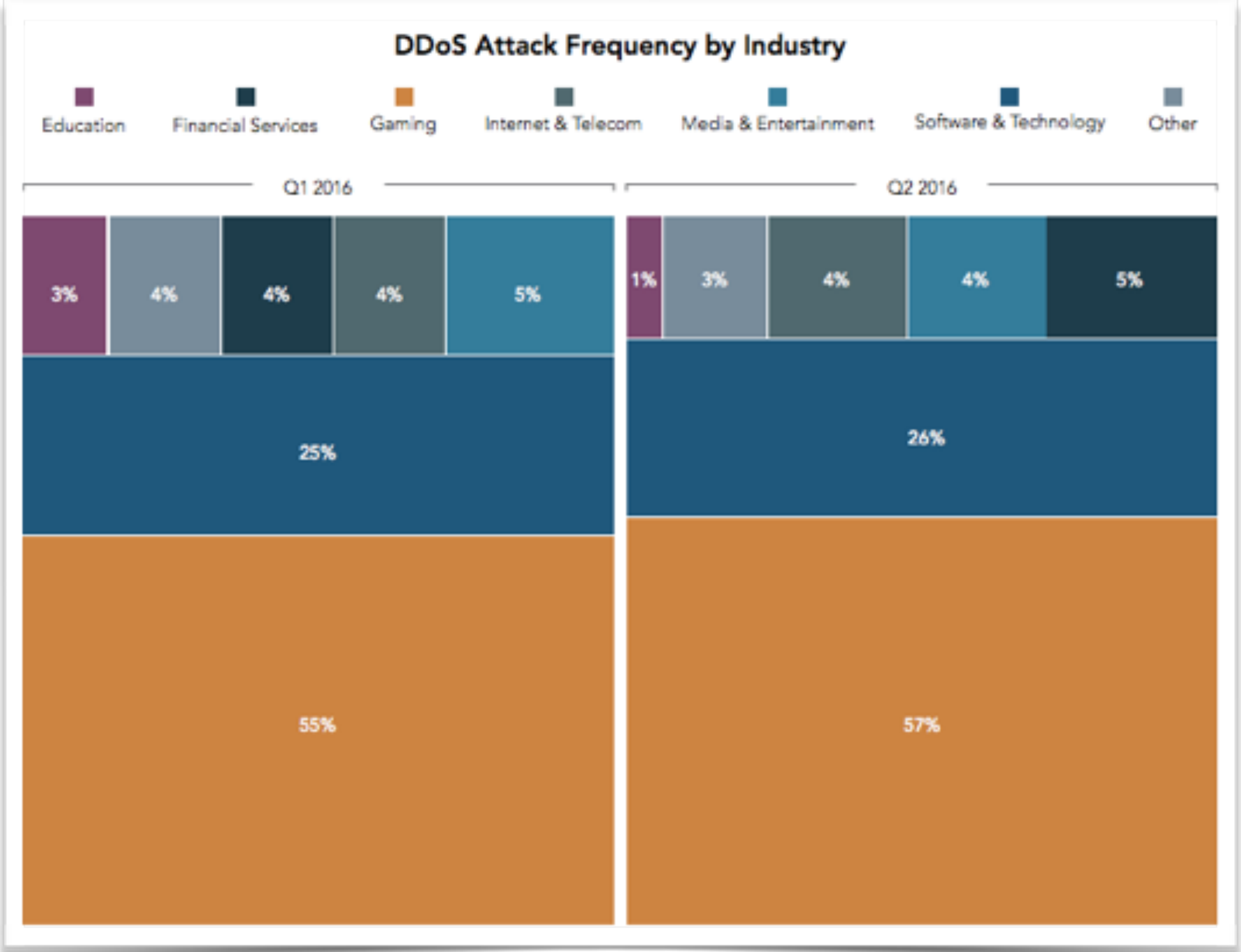
State of the Internet Security Report by Akamai

Statistics on DDos



Top 10 Source Countries for DDoS Attacks, Q2 2016

China	56.09%
US	17.38%
Taiwan	5.22%
Canada	3.77%
Vietnam	3.70%
Brazil	2.96%
Spain	2.94%
Singapore	2.90%
Italy	2.65%
UK	2.38%



DDoS Attack Frequency by Industry

State of the Internet Security Report by Akamai

DDos Prevention

- Keep your software up-to-date
- Know your network and services
  - Make inventory on a regular basis
  - Monitor
- Don’t make enemies and avoid becoming a target

DDos Prevention

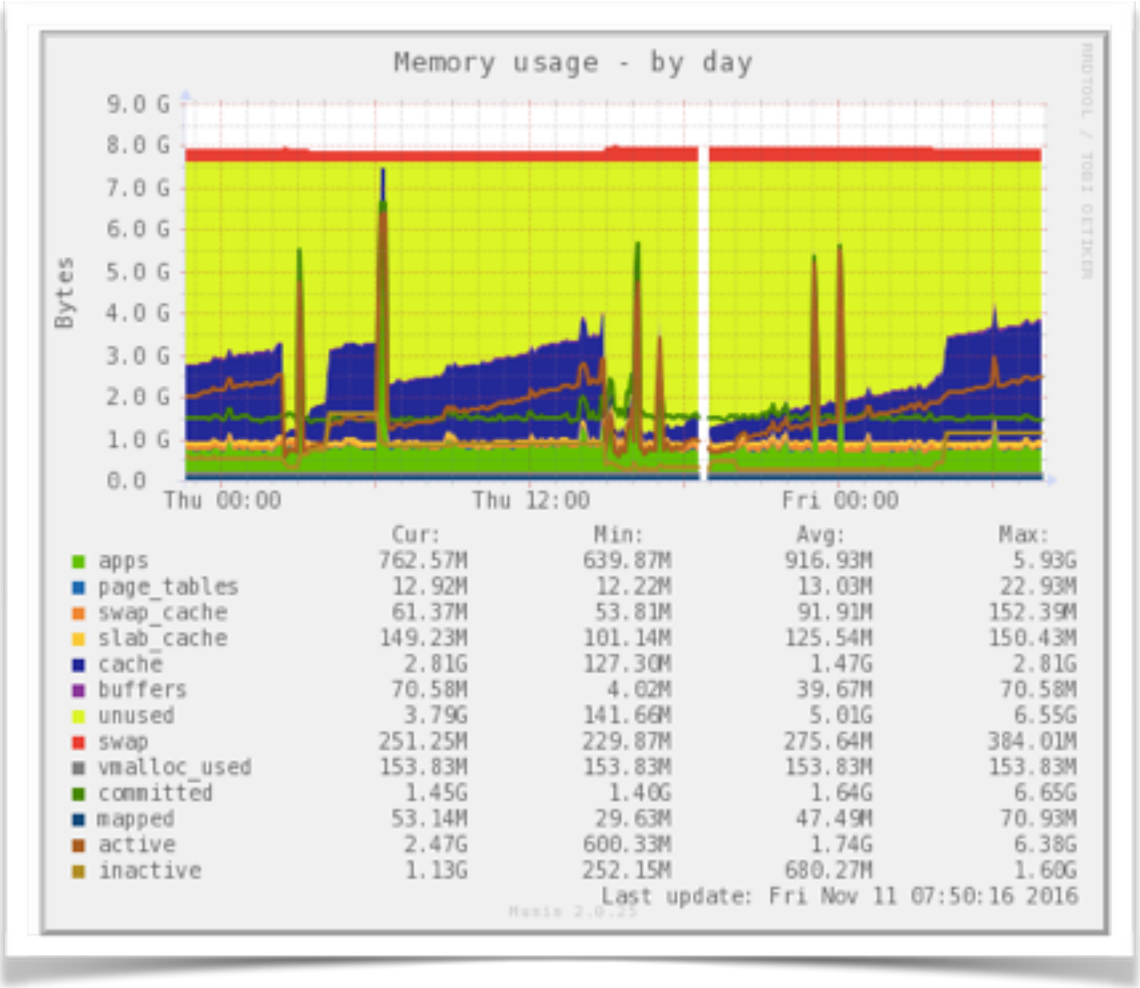
- Recommendations by the Dutch government
  - Make an overview and monitor your infrastructure
  - Check with each of your third-party suppliers to find out which (D)DoS countermeasures are in place and what the relevant contractual agreements are
  - Find out which countermeasures have been taken to protect your in-house infrastructure and take additional steps, if necessary
  - **Prepare your incident response** and think about **failover** scenarios for your online services
  - **Prepare a communication strategy**

DDos Prevention

- Ingress filtering (BCP38)
- RPKI
- BGPSEC

DDos Mitigation

- Detection!!!
  - You need to be able to detect an attack
  - Popular service vs. attack

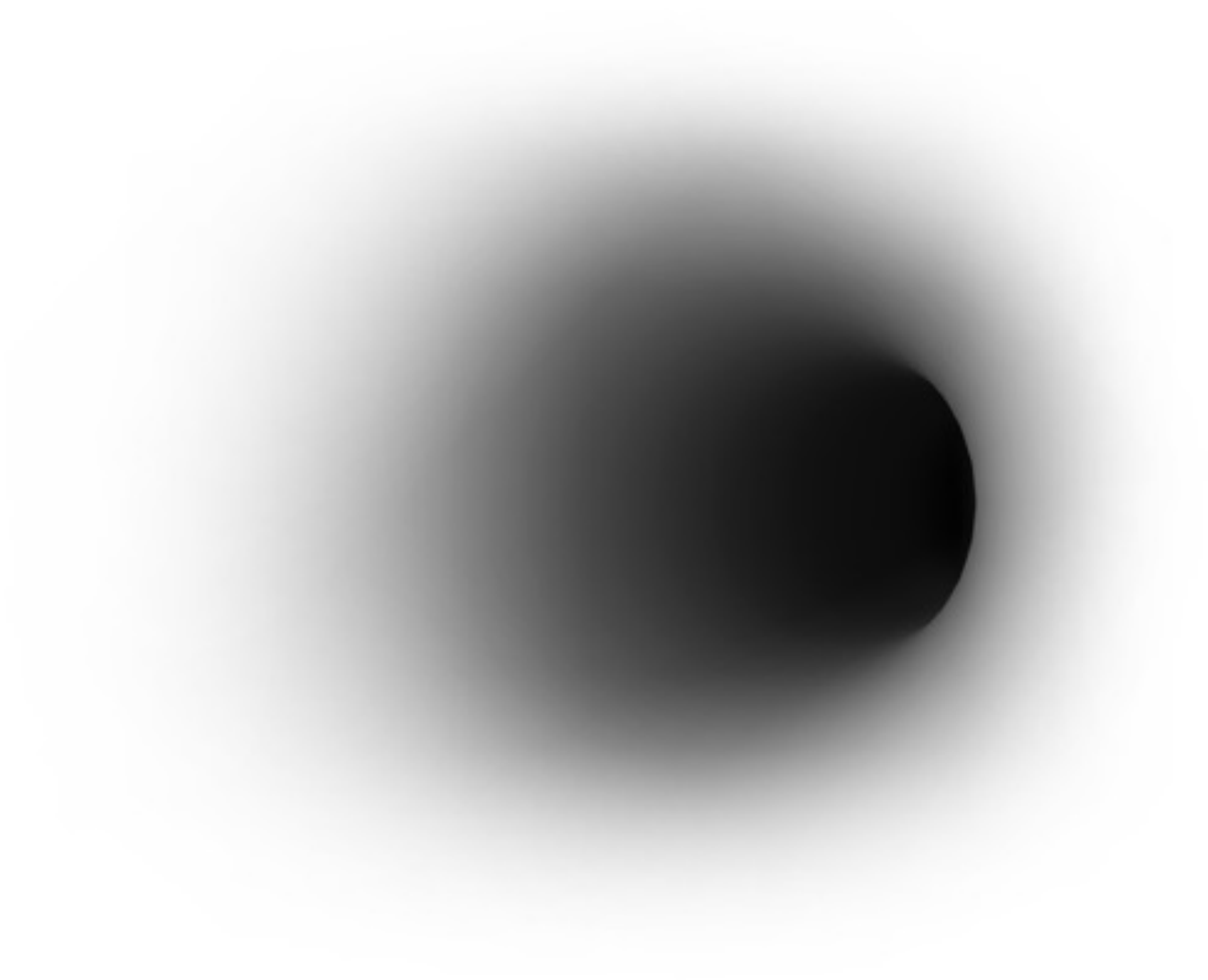


	Cur:	Min:	Avg:	Max:
🟩 apps	762.57M	639.87M	916.93M	5.93G
🟦 page_tables	12.92M	12.22M	13.03M	22.93M
🟧 swap_cache	61.37M	53.81M	91.91M	152.39M
🟨 slab_cache	149.23M	101.14M	125.54M	150.43M
🟦 cache	2.81G	127.30M	1.47G	2.81G
🟪 buffers	70.58M	4.02M	39.67M	70.58M
🟨 unused	3.79G	141.66M	5.01G	6.55G
🟥 swap	251.25M	229.87M	275.64M	384.01M
⬛ vmalloc_used	153.83M	153.83M	153.83M	153.83M
🟩 committed	1.45G	1.40G	1.64G	6.65G
🟦 mapped	53.14M	29.63M	47.49M	70.93M
🟫 active	2.47G	600.33M	1.74G	6.38G
🟫 inactive	1.13G	252.15M	680.27M	1.60G

Last update: Fri Nov 11 07:50:16 2016

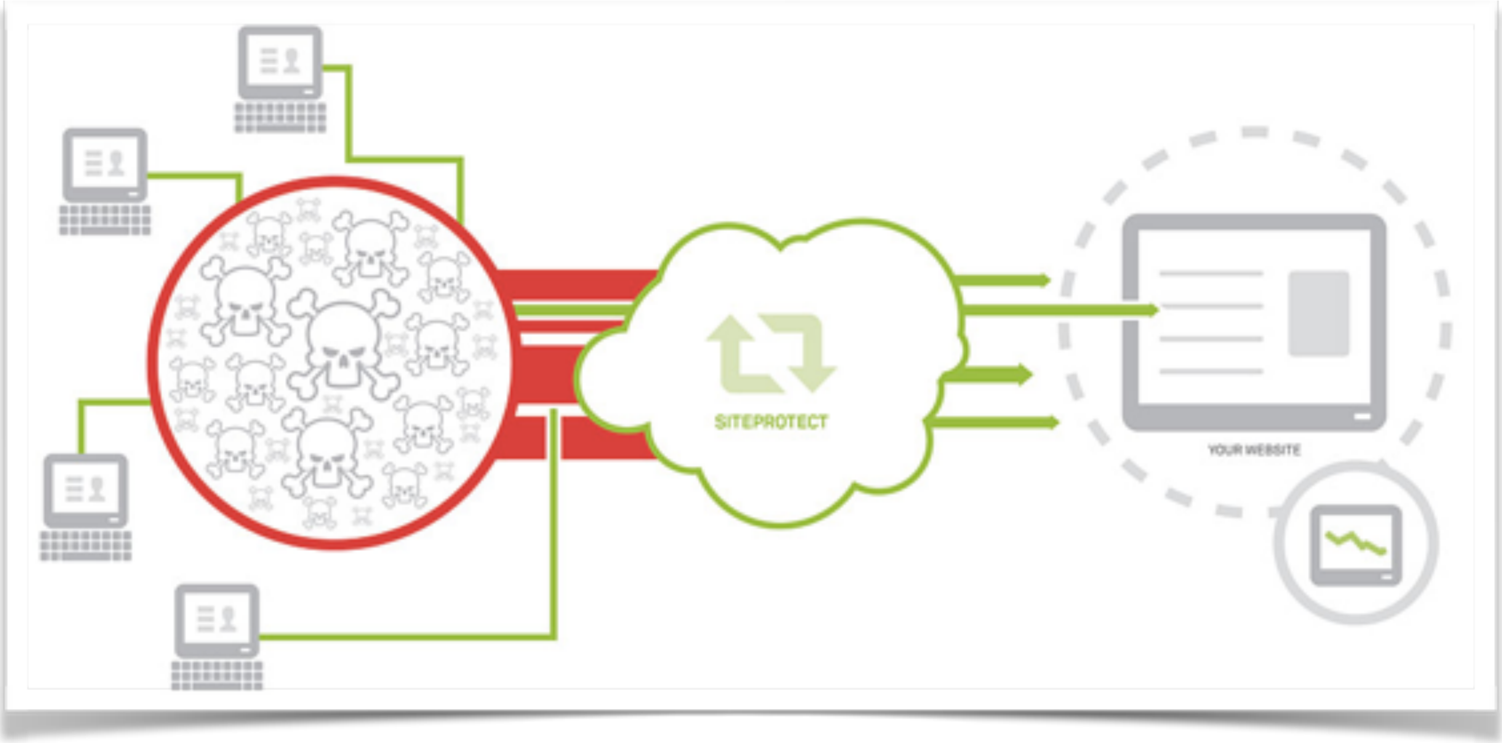
DDos Mitigation

- BGP blackholing



DDos Mitigation

- Traffic Scrubbing
  - Services like NaWas



https://www.neustar.biz/resources/product-literature/siteprotect-ddos-mitigation-failover-service

DDos Mitigation

- Spread the word and inform the right people
  - Abuse-c
  - National CERTs
  - Affected companies

DDos Mitigation

- Spread it even further
- Working Group mailing list
  - Routing WG
  - Anti-Abuse WG
- NOG/National lists
  - NANOG
  - NLNOG, DENOG, PLNOG, SWINOG, etc.
  - MKNOG?

Questions

christian.teuschel@ripe.net
@cteuschel