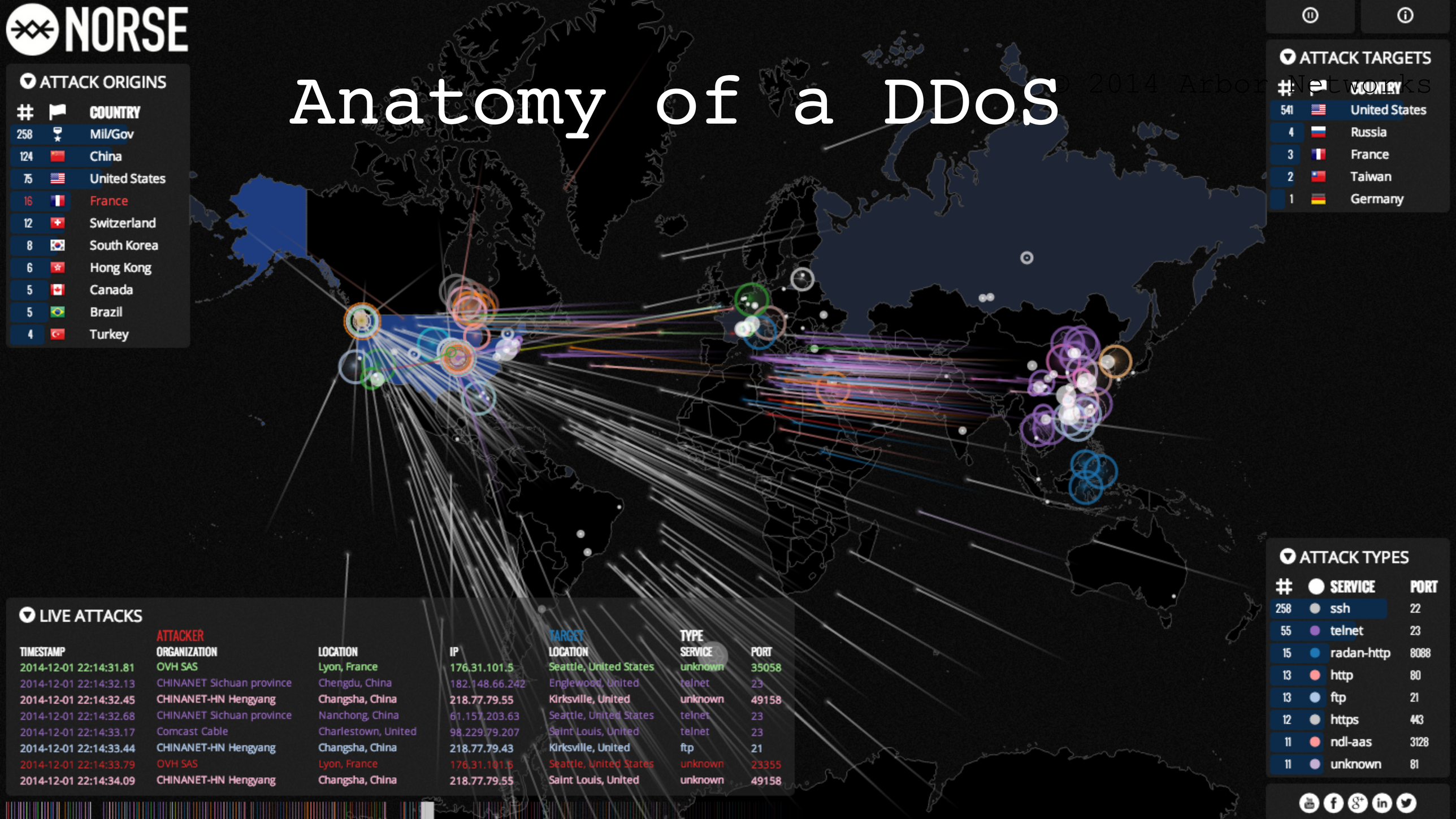

NORSE
Anatomy of a DDoS
© 2014 Arbor Networks
ATTACK ORIGINS
COUNTRY
258 Mil/Gov
124 China
75 United States
16 France
12 Switzerland
8 South Korea
6 Hong Kong
5 Canada
5 Brazil
4 Turkey
ATTACK TARGETS
COUNTRY
541 United States
4 Russia
3 France
2 Taiwan
1 Germany
LIVE ATTACKS
ATTACKER TARGET TYPE
TIMESTAMP ORGANIZATION LOCATION IP LOCATION SERVICE PORT
2014-12-01 22:14:31.81 OVH SAS Lyon, France 176.31.101.5 Seattle, United States unknown 35058
2014-12-01 22:14:32.13 CHINANET Sichuan province Chengdu, China 182.148.66.242 Englewood, United telnet 23
2014-12-01 22:14:32.45 CHINANET-HN Hengyang Changsha, China 218.77.79.55 Kirksville, United unknown 49158
2014-12-01 22:14:32.68 CHINANET Sichuan province Nanchong, China 61.157.203.63 Seattle, United States telnet 23
2014-12-01 22:14:33.17 Comcast Cable Charlestown, United 98.229.79.207 Saint Louis, United telnet 23
2014-12-01 22:14:33.44 CHINANET-HN Hengyang Changsha, China 218.77.79.43 Kirksville, United ftp 21
2014-12-01 22:14:33.79 OVH SAS Lyon, France 176.31.101.5 Seattle, United States unknown 23355
2014-12-01 22:14:34.09 CHINANET-HN Hengyang Changsha, China 218.77.79.55 Saint Louis, United unknown 49158
ATTACK TYPES
SERVICE PORT
258 ssh 22
55 telnet 23
15 radan-http 8088
13 http 80
13 ftp 21
12 https 443
11 ndl-aas 3128
11 unknown 81

Huh?

DDoS Attack

Distributed Denial of Service attack, the act of intentionally flooding a given computer network service to prevent normal access.


Aaron Kalin
He/Him


@martinisoft


Aaron Kalin
He/Him

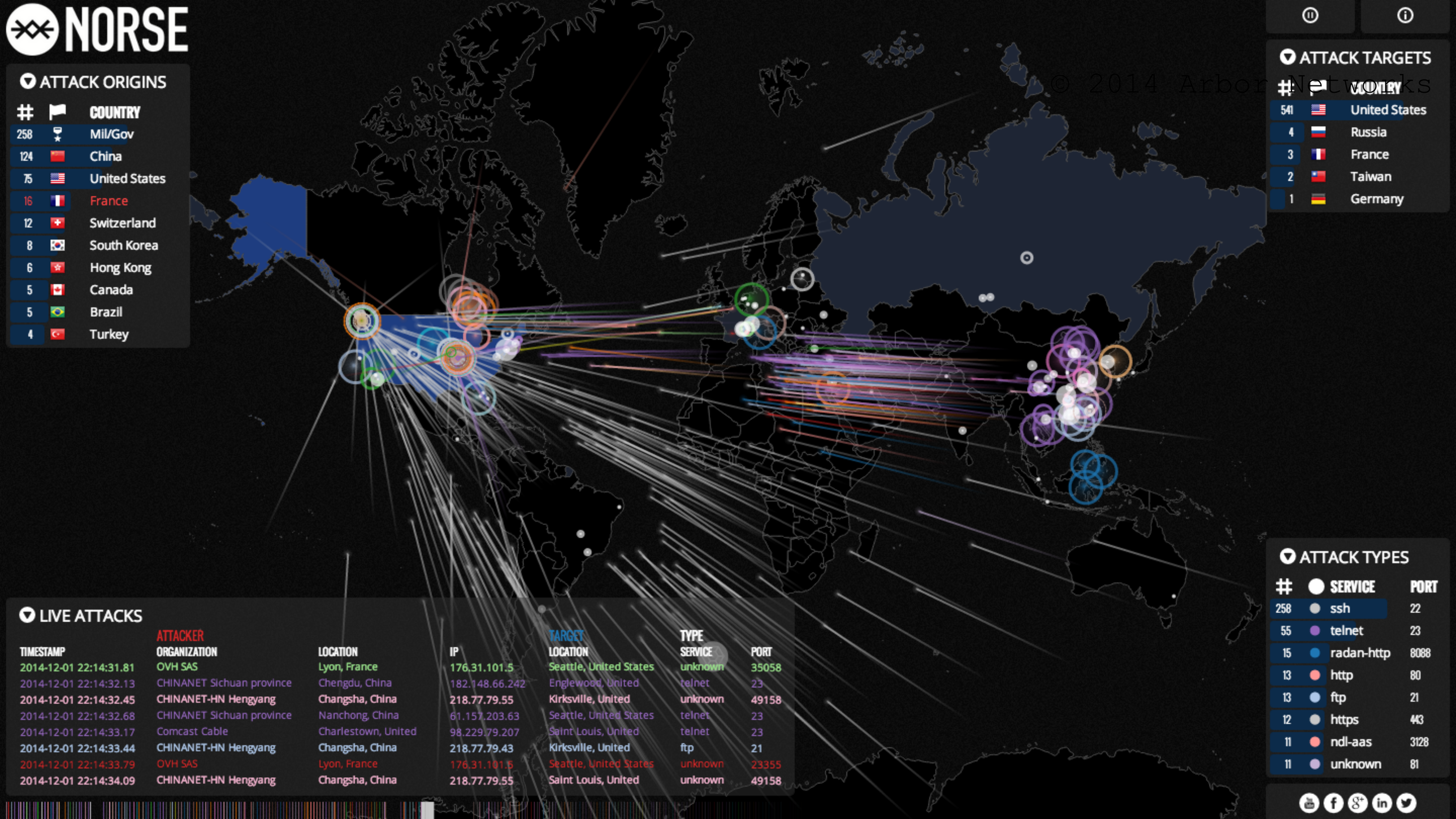

@martinisoft


Aaron Kalin
He/Him


TK-688

dnsimple

December 1st, 2014


NORSE
ATTACK ORIGINS
COUNTRY
258 Mil/Gov
124 China
75 United States
16 France
12 Switzerland
8 South Korea
6 Hong Kong
5 Canada
5 Brazil
4 Turkey
ATTACK TARGETS
COUNTRY
541 United States
4 Russia
3 France
2 Taiwan
1 Germany
© 2014 Arbor Networks
ATTACK TYPES
SERVICE PORT
258 ssh 22
55 telnet 23
15 radan-http 8088
13 http 80
13 ftp 21
12 https 443
11 ndl-aas 3128
11 unknown 81
LIVE ATTACKS
ATTACKER TARGET TYPE
TIMESTAMP ORGANIZATION LOCATION IP LOCATION SERVICE PORT
2014-12-01 22:14:31.81 OVH SAS Lyon, France 176.31.101.5 Seattle, United States unknown 35058
2014-12-01 22:14:32.13 CHINANET Sichuan province Chengdu, China 182.148.66.242 Englewood, United telnet 23
2014-12-01 22:14:32.45 CHINANET-HN Hengyang Changsha, China 218.77.79.55 Kirksville, United unknown 49158
2014-12-01 22:14:32.68 CHINANET Sichuan province Nanchong, China 61.157.203.63 Seattle, United States telnet 23
2014-12-01 22:14:33.17 Comcast Cable Charlestown, United 98.229.79.207 Saint Louis, United telnet 23
2014-12-01 22:14:33.44 CHINANET-HN Hengyang Changsha, China 218.77.79.43 Kirksville, United ftp 21
2014-12-01 22:14:33.79 OVH SAS Lyon, France 176.31.101.5 Seattle, United States unknown 23355
2014-12-01 22:14:34.09 CHINANET-HN Hengyang Changsha, China 218.77.79.55 Saint Louis, United unknown 49158

40Gbit Burst of Traffic

40Gbit Burst of Traffic
25Gbit Sustained Traffic

40Gbit Burst of Traffic
25Gbit Sustained Traffic
50Million Packets Per Second at Peak

Duration: 8 hours

How did it happen?

How did it happen?

Earlier That Day…

Earlier That Day…

New trial signup

Earlier That Day…

New trial signup

Had several domains, one of them was actively being attacked

Shooting the Messenger

Shooting the Messenger

We were now the authoritative DNS resolver for a website being attacked. :(

$ bundle install

Fetching gem metadata from
https://rubygems.org/..

Protocols attacked

Protocols attacked

DNS

Protocols attacked

DNS

ICMP

Protocols attacked

DNS

ICMP

NTP

Protocols attacked

DNS

ICMP

NTP

HTTP

Why?

Competitor Sabotage

Make your competition look bad by inducing downtime of their services

Revenge

Got fired from your job? Why not DDoS your former employer?

Blackmail

Give me $10,000 or your site gets it!

Anti-Propaganda

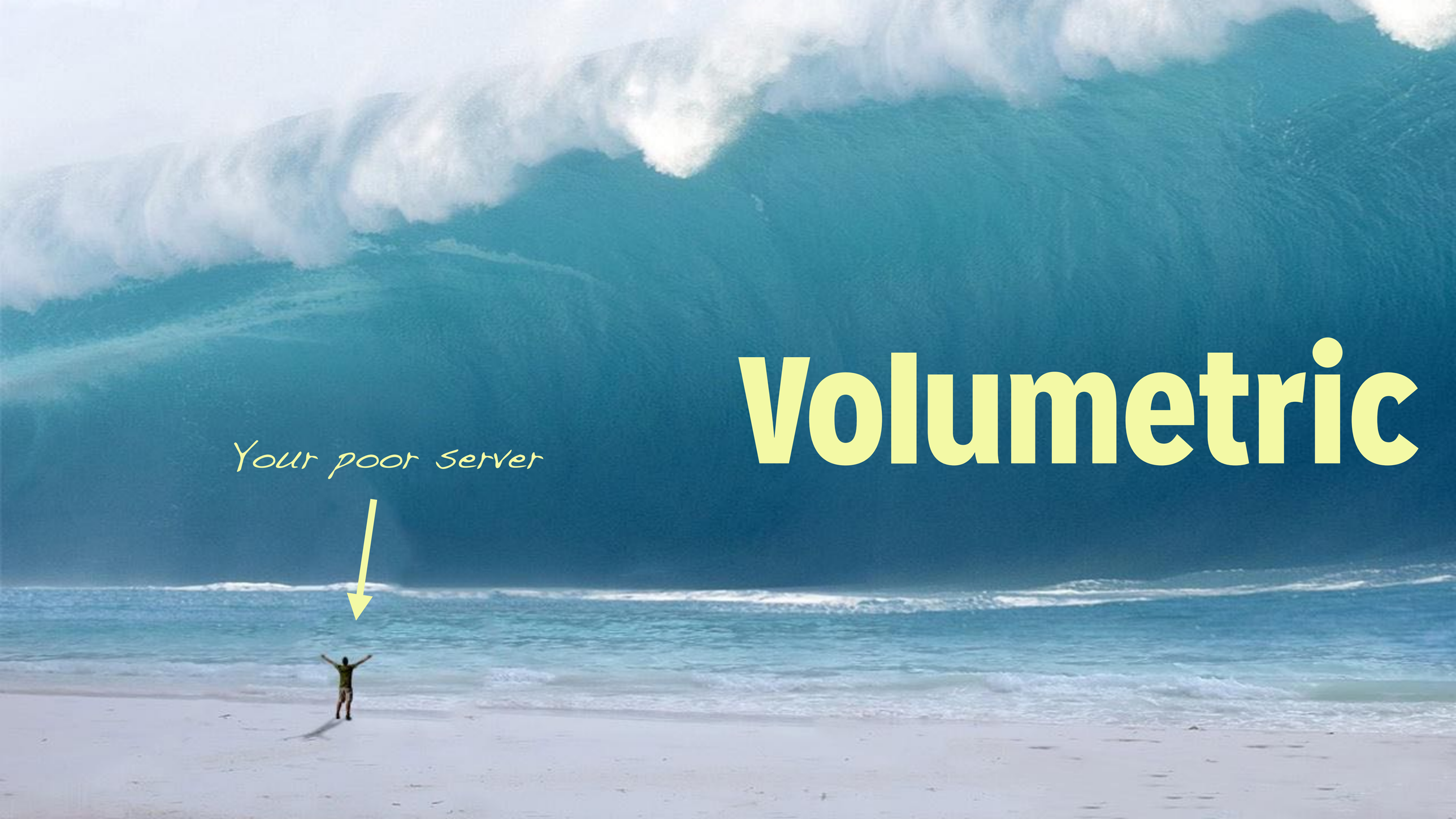
Hosting some anti-government content?
You need to be silenced!

The Lulz

A fun party trick, proving a point to your friends, or silencing outspoken feminists.

What types of attacks are out there?


Volumetric


Volumetric
Your poor server

Application

Resource Exhaustion

Photo Credit: Wolfman3000


How would you attack
DNS?

Amplification attack (DNS)

Amplification attack (DNS)

64byte query results in a ~3Kilobyte answer

Amplification attack (DNS)

64byte query results in a ~3Kilobyte answer

50x return on a single packet

Amplification attack (DNS)

64byte query results in a ~3Kilobyte answer

50x return on a single packet

Spamhaus attack (300Gbit) was carried out by one person with a laptop...

Amplification attack (NTP)

Amplification attack (NTP)

Send a forged ‘monlist’ request to ask for the last 600 systems to ask for the time

Amplification attack (NTP)

Send a forged ‘monlist’ request to ask for the last 600 systems to ask for the time

555x return on a single packet

TCP SYN Flood

TCP SYN Flood

Open a ton of half-open TCP connections to block out legitimate DNS requests (not all of them are UDP)

Randomization

New style of attack that has surfaced. Randomize the subdomains of a known domain in order to bust DNS query caches and overload processing power of a DNS server.


Totally not a virus. Trust me...im a dolphin
SEEMS LEGIT
ROFLBOT

Compromised Servers or Credentials

Compromised Servers or Credentials

Infect a server or computer with remote-control software to attack a target.

Compromised Servers or Credentials

Infect a server or computer with remote-control software to attack a target.

Use someone’s mistakenly posted AWS keys to create new attack servers.

Infected IoT Devices

Infected IoT Devices

The recent DynDNS attack was carried out by Internet of Things (IoT) devices infected with the Mirai malware.

Browser Injection Attacks

Get a browser to run code that attacks a target. Simple as infecting links or phishing emails that trick someone into running malicious code.


Can you
defend
against
them?
Copyright 2016 Home Box Office

Mostly…

Secondary DNS

Secondary DNS

Pro: Backup DNS in case your primary DNS goes down

Secondary DNS

Pro: Backup DNS in case your primary DNS goes down

Con: Limited support, can only setup one additional DNS provider

Anycast

Anycast

Pro: One address, multiple locations.

Anycast

Pro: One address, multiple locations.

Con: Extremely difficult and expensive to setup. Sharing state between multiple locations is hard.

Network Planning

Network Planning

Use multiple network switches, routers, and providers to segment traffic

Network Planning

Use multiple network switches, routers, and providers to segment traffic

More targets to hit means a bigger attack is required for volumetric attacks

DDoS Defense Hardware

DDoS Defense Hardware

Pro: Specialized hardware to detect common attack patterns

DDoS Defense Hardware

Pro: Specialized hardware to detect common attack patterns

Con: Extremely expensive, also did not work for us :(

DDoS Defense Services

DDoS Defense Services

Pro: Quick and easy to setup

DDoS Defense Services

Pro: Quick and easy to setup

Con: Typically relies on caching, your dynamic site will not work well behind their system

https://commons.wikimedia.org/wiki/User:Famartin

Where do we go from here?

Attacks will likely get worse and increase in size as the internet continues to grow

It’s a cat and mouse game similar to Computer Viruses and Anti-Viruses

More distributed services for things like DNS might be an answer

https://www.flickr.com/photos/doxieone/6079559391

Thank you

@martinisoft

Resources

Cloudflare DDoS Protection - https://www.cloudflare.com/ddos

Project Galileo - https://www.cloudflare.com/galileo

Attack Map - http://map.norsecorp.com/

How DNS Works - http://howdns.works

Want to try DNSimple? - https://dnsimple.com/o/aaron

Like my driving? - Tweet @martinisoft and/or send feedback to the EventsXD app.