Denial of Service

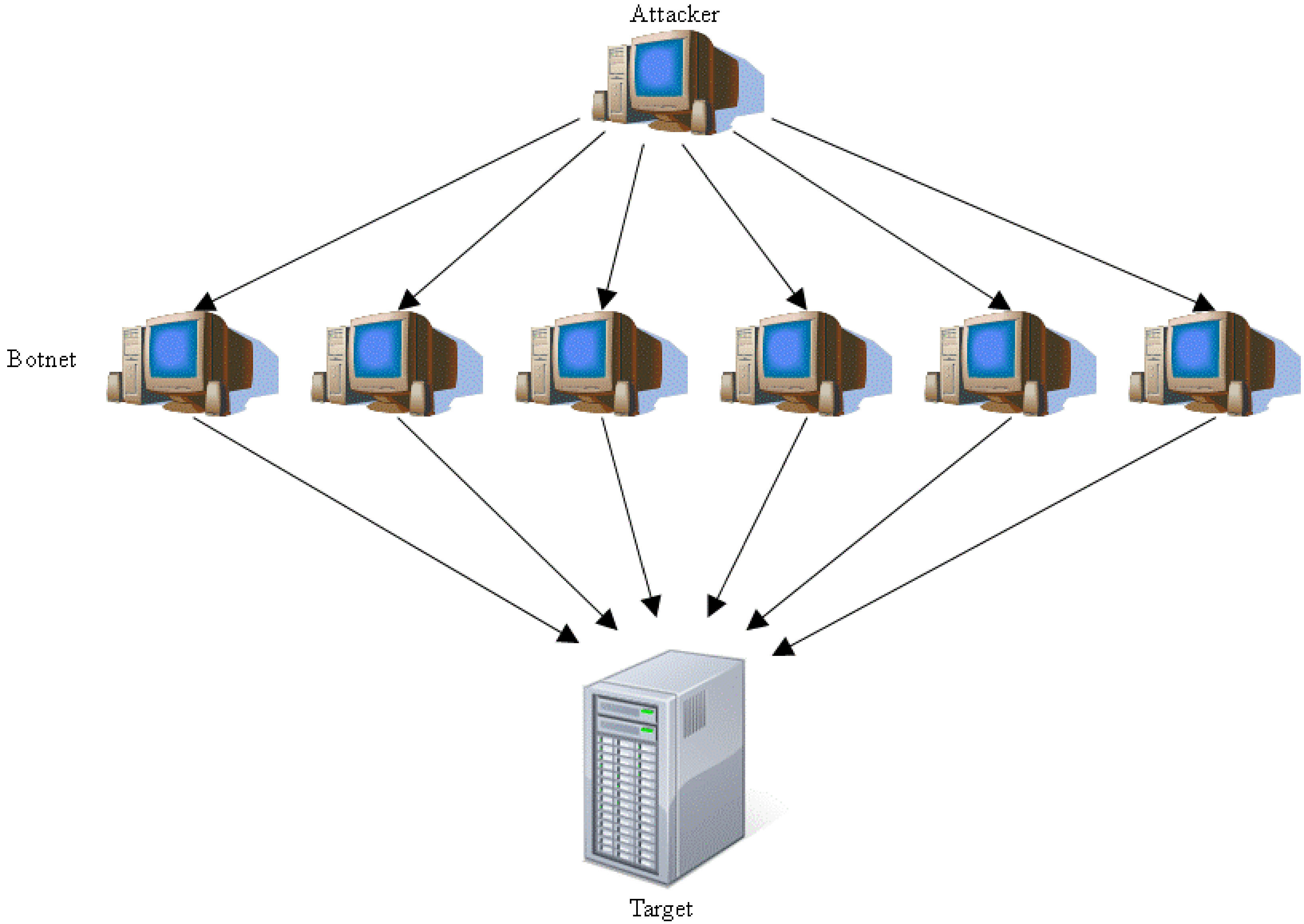
Ronald Osure

KENET Cyber Security Training
October 26th - 30th 2015

Agenda

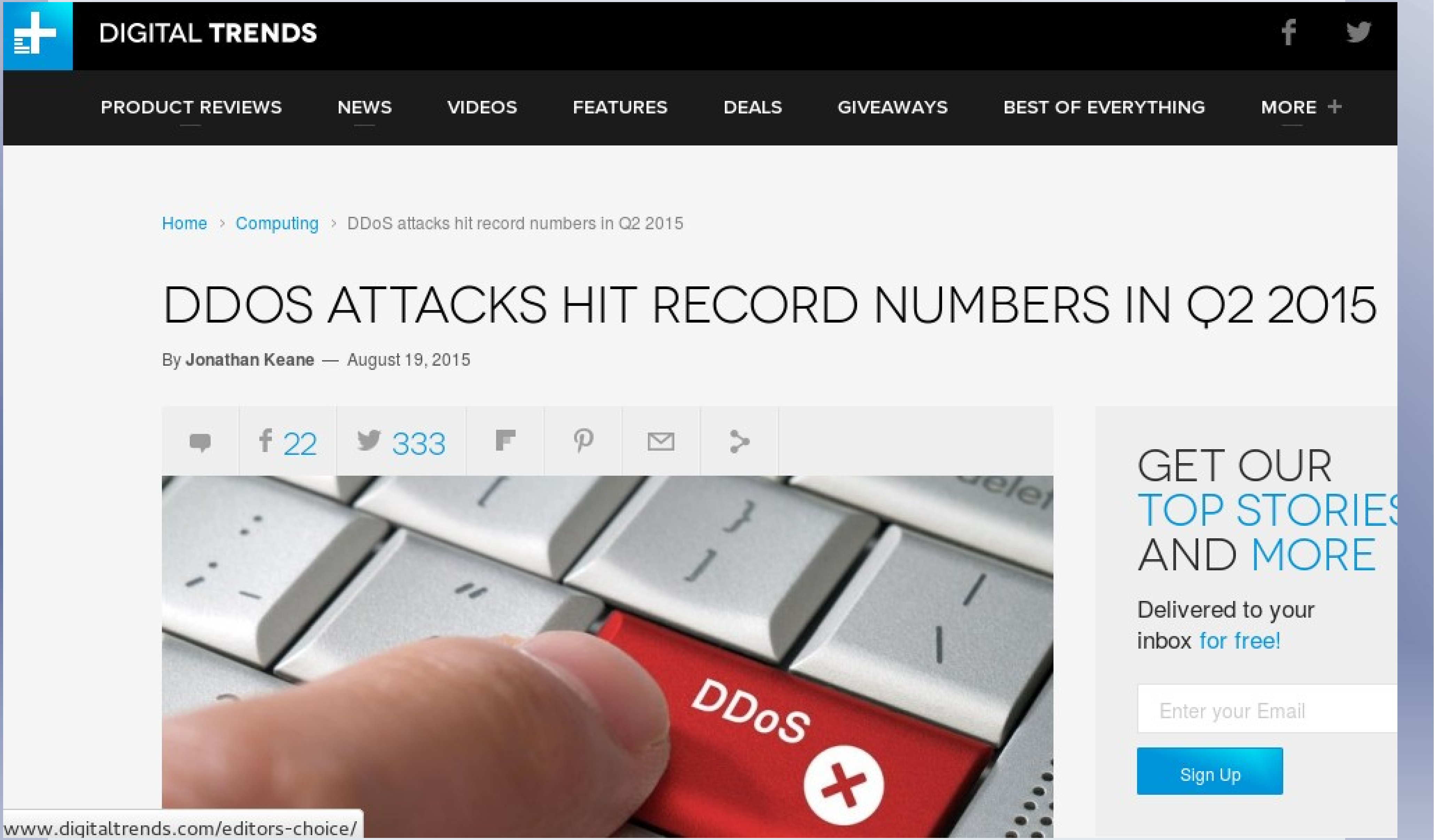
- What is (D)DOS?
- Whats recent
- Symptoms of DOS
- DOS Attack techniques
- DOS Countermeasure

Figure 1 DDoS attack



Attacker sends command to botnet, botnet floods server with messages

Denial-of-service (DoS) is an attack that prevents authorized users from accessing a computer or network



Home › Computing › DDoS attacks hit record numbers in Q2 2015

DDOS ATTACKS HIT RECORD NUMBERS IN Q2 2015

By **Jonathan Keane** — August 19, 2015

GET OUR TOP STORIES AND MORE

Delivered to your inbox for free!

http://www.digitaltrends.com/computing/ddos-attacks-hit-record-numbers-in-q2-2015/

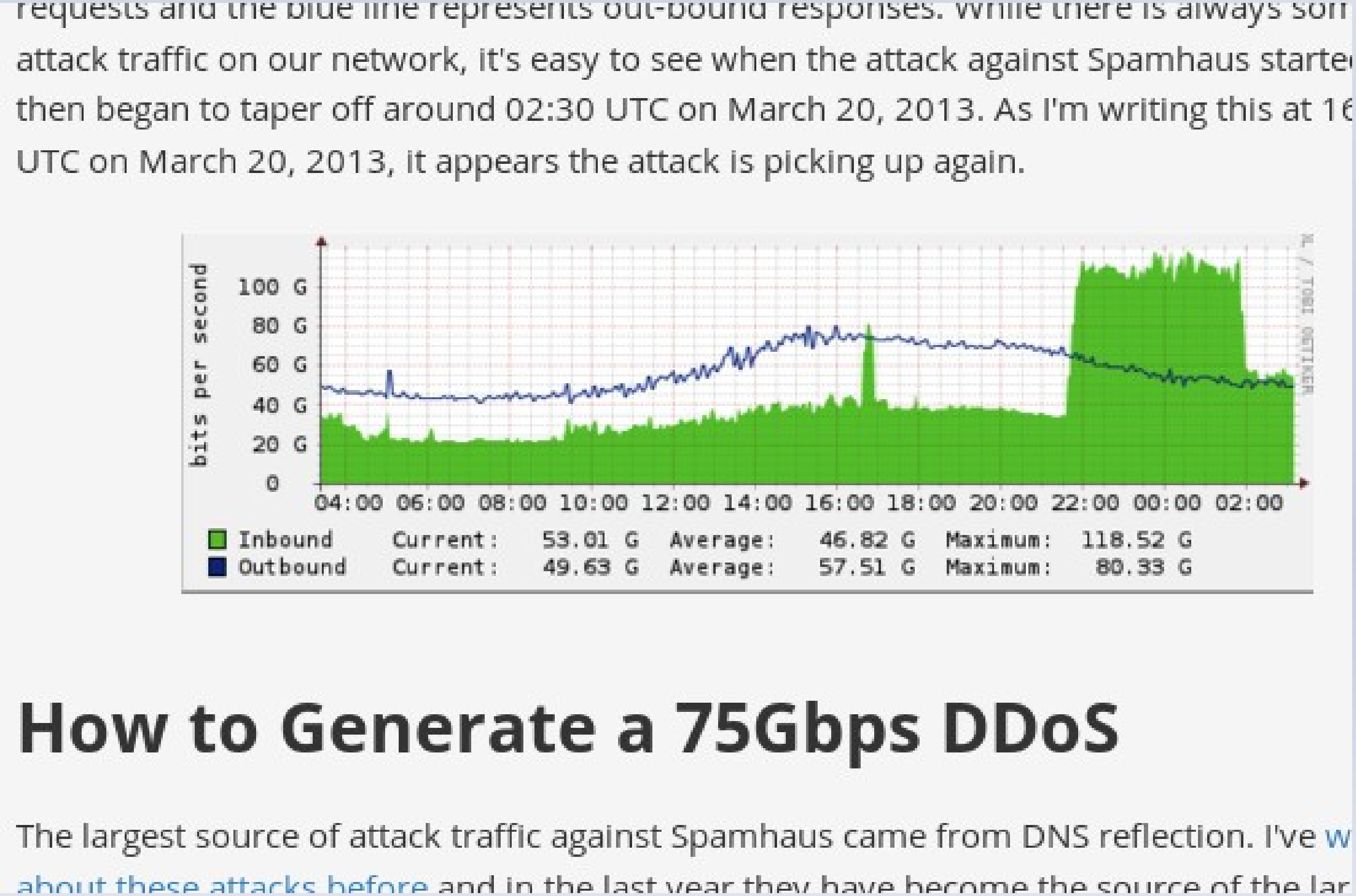
Akamai’s State of the Internet report has confirmed that DDoS attacks have spiked by six percent from the **2nd Quarter 2015**. Staggeringly, the number of attacks have gone up a mind-boggling **132** percent, compared to the same quarter last year, reports Security Magazine.

In the same quarter:

- There were 12 attacks that pushed beyond 100 GbpS (gigabits per second).
- The largest attack measured was a ridiculously high 240 Gbps and lasted for more than 13 hours.
- Akamai also added that it recorded the highest packet rate attacks, peaking at 214 million packets per second.
- Furthermore, average peak bandwidth went up 15.46 percent from Q1 this year.

https://lifars.com/2015/08/ddos-attacks-are-stronger-more-in-number-than-ever/

DdoS that knocked Spamhaus offline



requests and the blue line represents out-bound responses. While there is always som attack traffic on our network, it's easy to see when the attack against Spamhaus starte then began to taper off around 02:30 UTC on March 20, 2013. As I'm writing this at 16 UTC on March 20, 2013, it appears the attack is picking up again.

🟩 Inbound	Current:	53.01 G	Average:	46.82 G	Maximum:	118.52 G
■ Outbound	Current:	49.63 G	Average:	57.51 G	Maximum:	80.33 G

How to Generate a 75Gbps DDoS

The largest source of attack traffic against Spamhaus came from DNS reflection. I've w about these attacks before and in the last year they have become the source of the lar

https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/

Symptoms of a DoS

- Unavailability of a particular website
- Inability to access any website
- Dramatic increase in the amount of emails received
- Unusually slow network performance

DoS attack techniques

- Bandwidth attacks
- Service request floods
- SYN flooding
- ICMP Flooding
- Peer-to-Peer attacks

DoS countermeasures

- Ingress filtering
- Egress filtering
- TCP intercept (fake connections)

References

- CEH
- *Other references inline in slides*

QUESTIONS ?