Latest Trends in DDoS Attacks

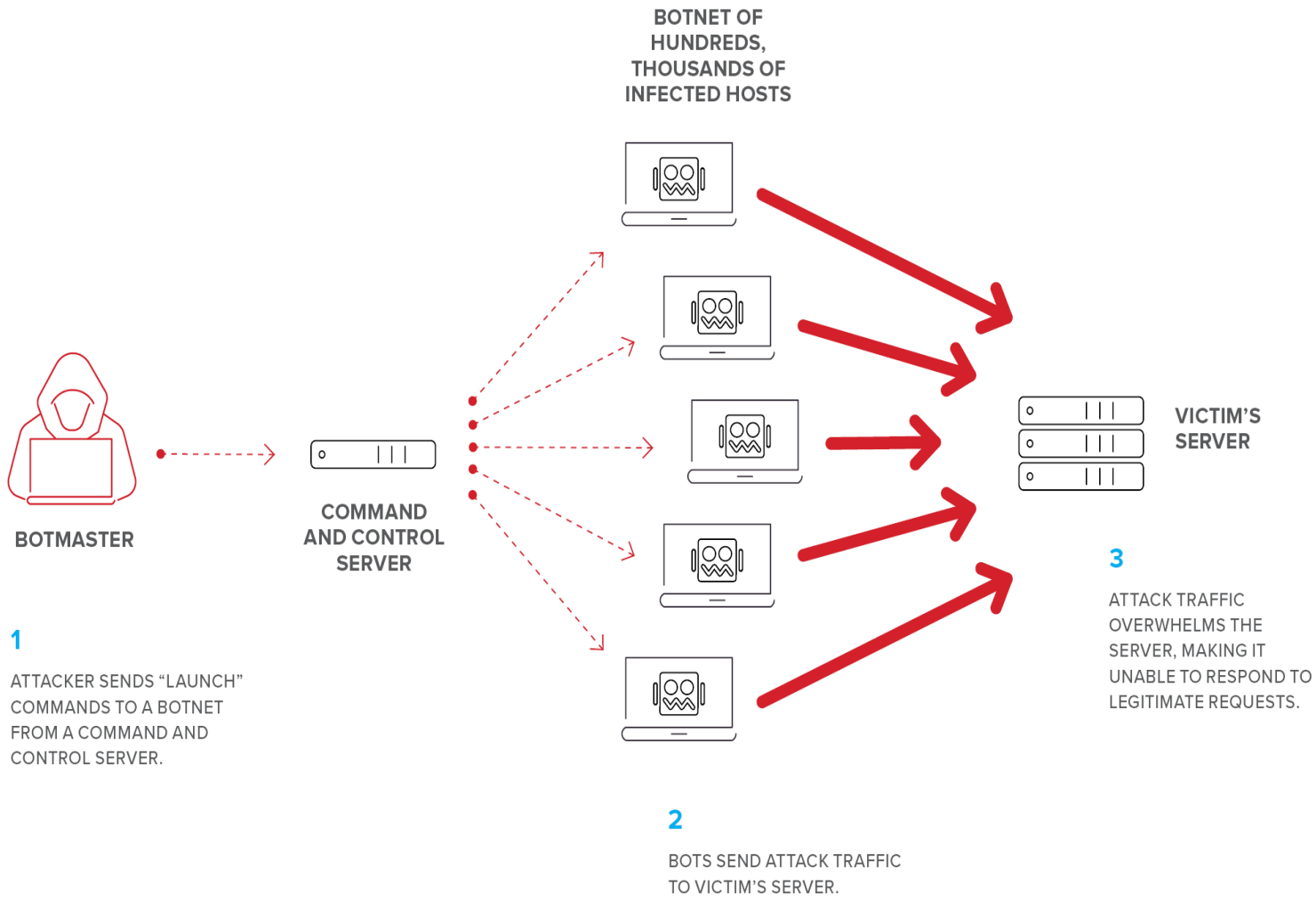
By: Aditya Sharma, Adham El Shafie, and Tiffany Alvear

What is a DDos Attack?

- **Distributed** Denial of Service
- **Multiple** compromised systems (usually infected with a Trojan) target a website/server etc.
- Make website/online service inoperable by **flooding it with more traffic than it can handle**

How does a DDos Attack work?

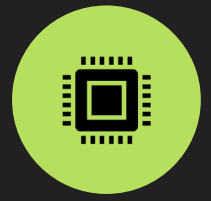
Botnets: armies of hundreds or thousands of Internet-connected computers (*zombies* or *bots*) that are infected with malware



https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service-attack-

Why is it concerning?

Exploit diversion of target's attention



Computer may be a botnet without knowing it

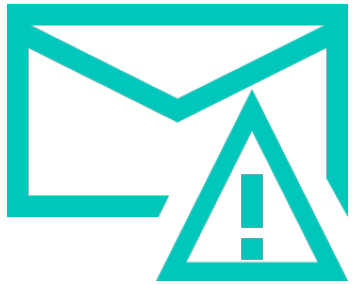
Symptoms hard to identify as being unusual

Types of DDos Attacks

Volume-based attacks	• The attack's goal is to saturate the bandwidth of the victims site. • Measured in bits per second (Bps).
Protocol attacks	• Attacks server resources and any intermediary devices (routers, gateways, firewalls, etc.). • Measured in packets per second (Pps).
Application Layer attacks	• Attacks done to crash the web server with legitimate GET/POST requests. • Magnitude is measured in Requests per second (Rps).

UDP Flood

Floods random ports on remote host to extract ICMP ‘Destination Unreachable’ replies. This takes up resources and makes the remote host almost inaccessible.



ICMP (Ping) Flood

Similar principle to the UDP flood but with ICMP (ping) requests that the remote host would reply to which takes up resources.

Volume Based Attacks (Bps)

Protocol Based Attacks (Pps)

SYN Flood

Multiple spoofed IP addresses initiating a 3-way handshake with the remote host. When there is no acknowledgement for the requests, the resources have been allocated already resulting in a DoS.

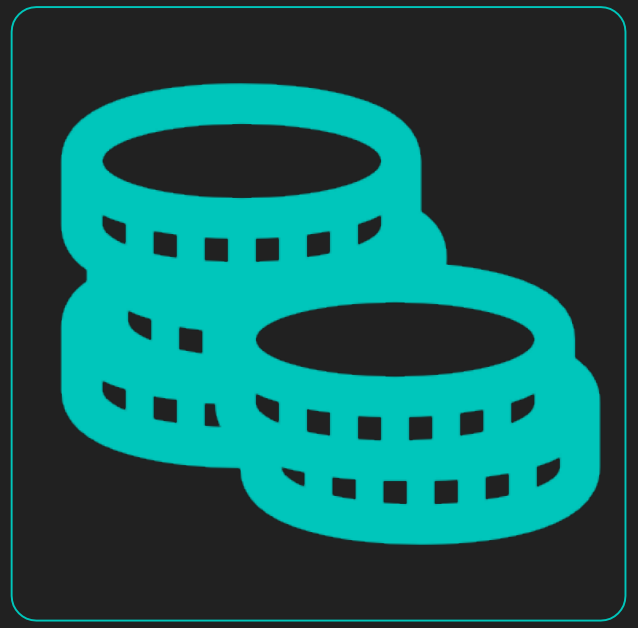
Ping of Death

Sending fragmented pings that are under the MTU limit but when the victim defragments the packet is over the maximum packet limit – 65,535 bytes – and can result in OS crashing.

Smurf Attack

Attacker sends a ping request to a broadcast IP address from a spoofed IP address as the source – the victim. The each of the IP addresses of the broadcasted address responds to the spoofed source address resulting in flooding victim with ICMP (ping) replies.

US Banks



- 2012
- Peak floods 60 Gbps of Traffic
- DNS packets
- Online and mobile banking became slow

GitHub

- Started March 26, 2015
- Lastest About 5 days
- Attacked 2 Projects called greatfire and cn-nytimes
- Chinese government is the assumed culprit
- Javascript made anyone on Baidu to request those projects
- Github attacked with millions of requests
- Packets also had different TTL

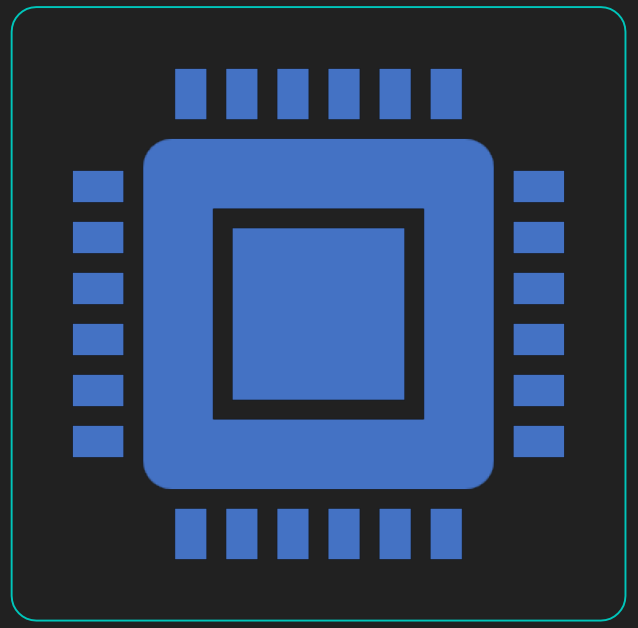
Github 2018

- 10-minute DDoS attack
- February 28th, 2018
- Estimated to be 1.35 terabits per second of traffic
- About 126.9 million packets per second
- Thousands of different autonomous systems(ASNs)
- The peak was caused by Memcached based attack

Imperva's client

- Another possible candidate for largest DDoS attack
- Jan 10, 2019
- SYN flood
- 580 million packets per second(PPS)

DYN



- Internet Infrastructure
- October 21st, 2016
- Botnets on printers, IP cameras, baby monitor etc
- Mirai malware used on those IoT
- DNS lookup from tens of millions of IP
- Masked TCP/UDP traffic over port 53
- 1.2 Tbps at peak

The Great False Attack

- Not All DDoS are intentional
- June 24th, 2016
- Automatic route Optimizing software used by DQE commination caused it
- Software told Border Gateway Protocol(BGP) that the route for some of the traffic is towards them by accident
- Millions of traffic diverted towards them
- Some of these traffics were for facebook, google

Wikipedia Attack

September 6,7 2019

Wikipedia was down in Germany and some other parts of Europe

- Most of the issues where in the connect phase of HTTP server
- computers would not be able to establish three-way TCP

AWS DDoS Attack

October 23rd, 2019

Lasted about 8 hours, 10:30 AM to 6:30 PM

Parts of AWS taken offline for hours

Digital Map Attack

https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18185&view=map

References

- https://arstechnica.com/information-technology/2015/03/massive-denial-of-service-attack-on-github-tied-to-chinese-government/
- https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/
- https://www.itproportal.com/news/aws-hit-by-ddos-attack/
- https://slate.com/technology/2019/06/verizon-dqe-outage-internet-cloudflare-reddit-aws.html
- https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html
- https://www.webopedia.com/TERM/D/DDoS_attack.html
- https://www.f5.com/labs/articles/education/what-is-a-distributed-denial-of-service
- https://github.blog/2018-03-01-ddos-incident-report/-attack-
- https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
- https://www.cio.com/article/2389721/ddos-attacks-against-us-banks-peaked-at-60-gbps.html
- https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/