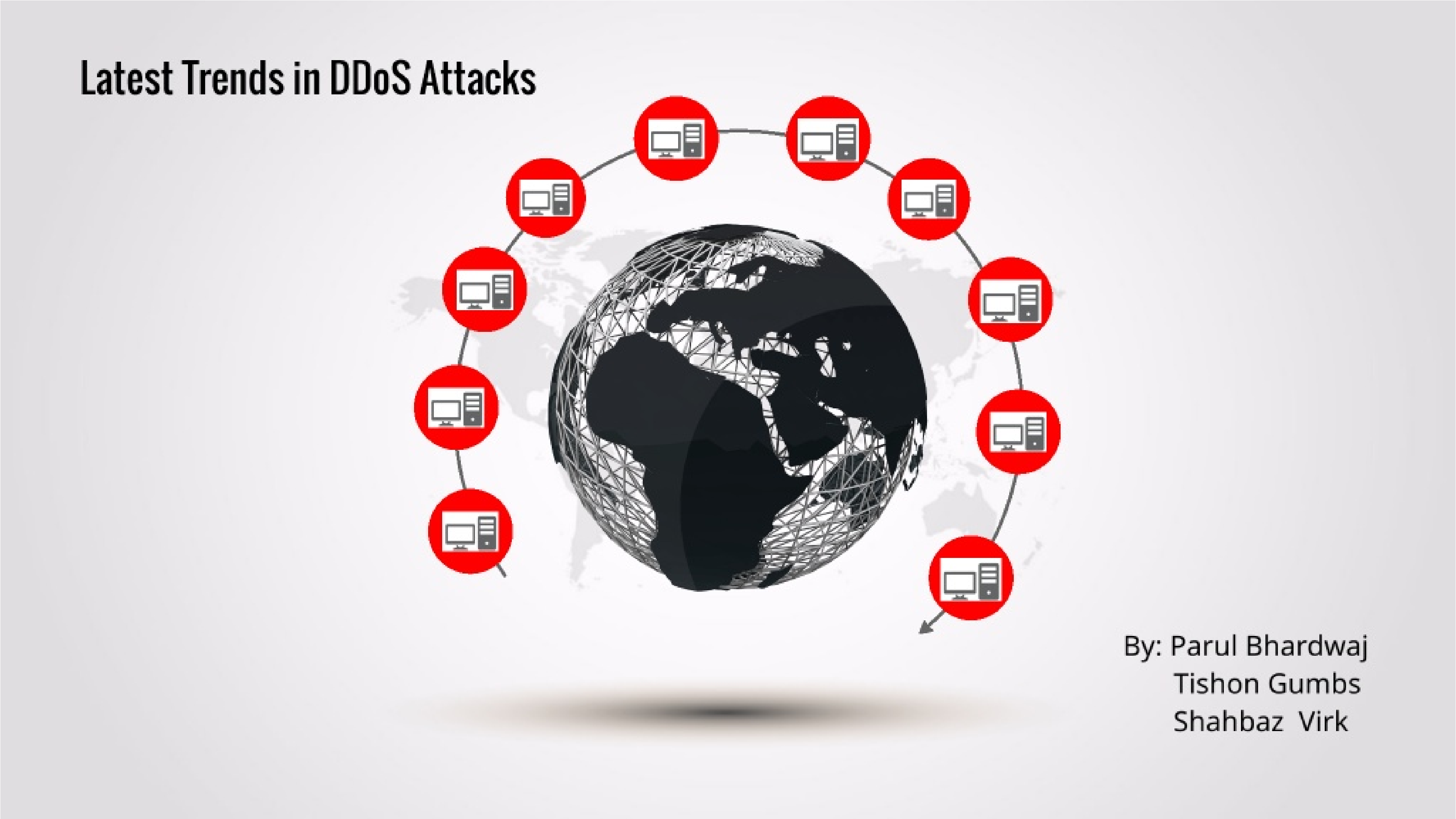


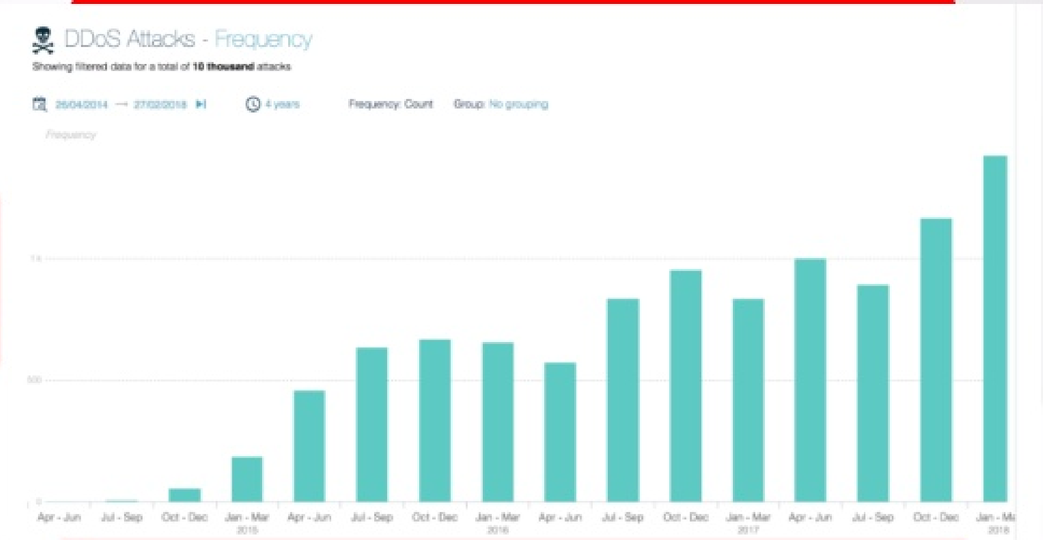
Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

DDoS Attack

Distributed Denial of Service

Attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web server.



DDoS Attacks - Frequency

Showing filtered data for a total of **10 thousand** attacks

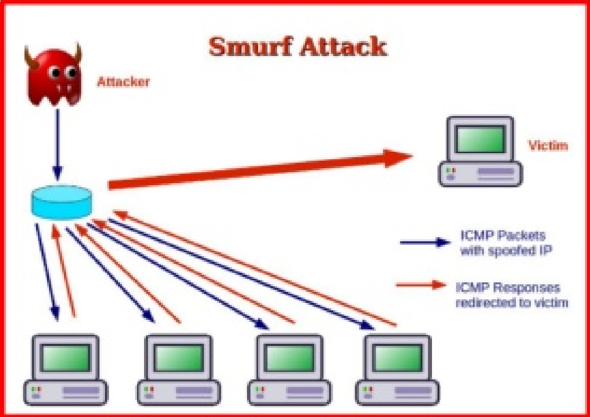
26/04/2014 → 27/02/2018 4 years Frequency: Count Group: No grouping

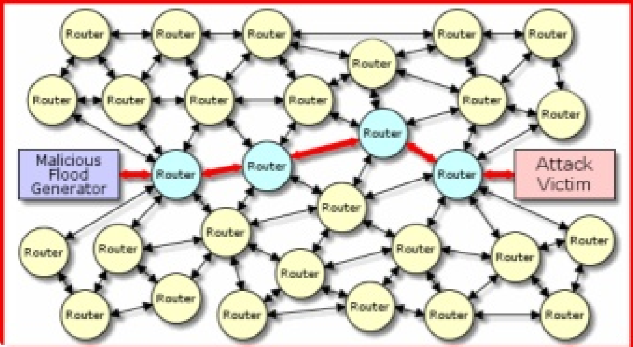
Latest Trends in DDoS Attacks

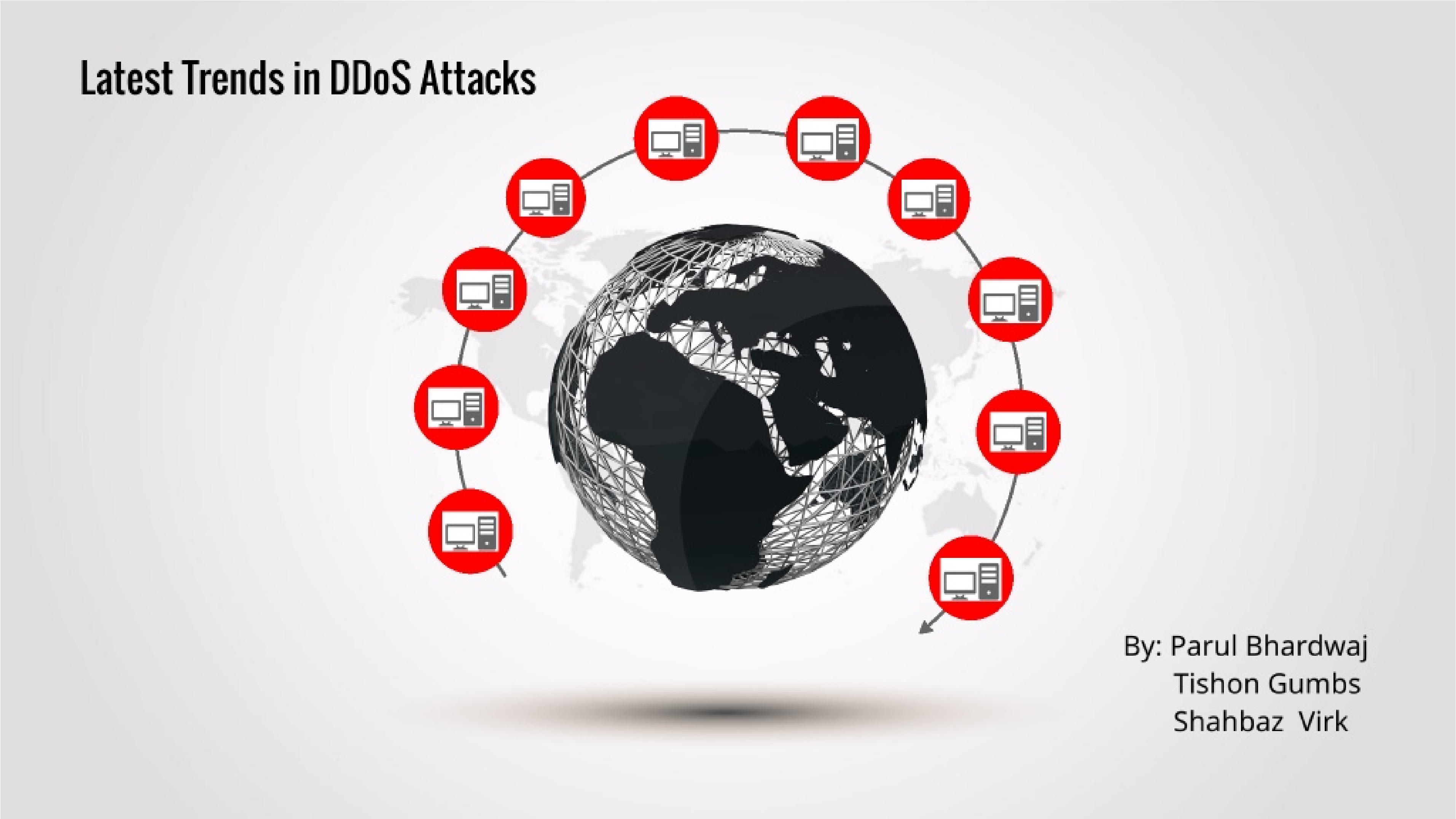
By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

Methods of Attack

- Smurf
- TCP
- Fragmentation
- Reflective
- Non-Reflective

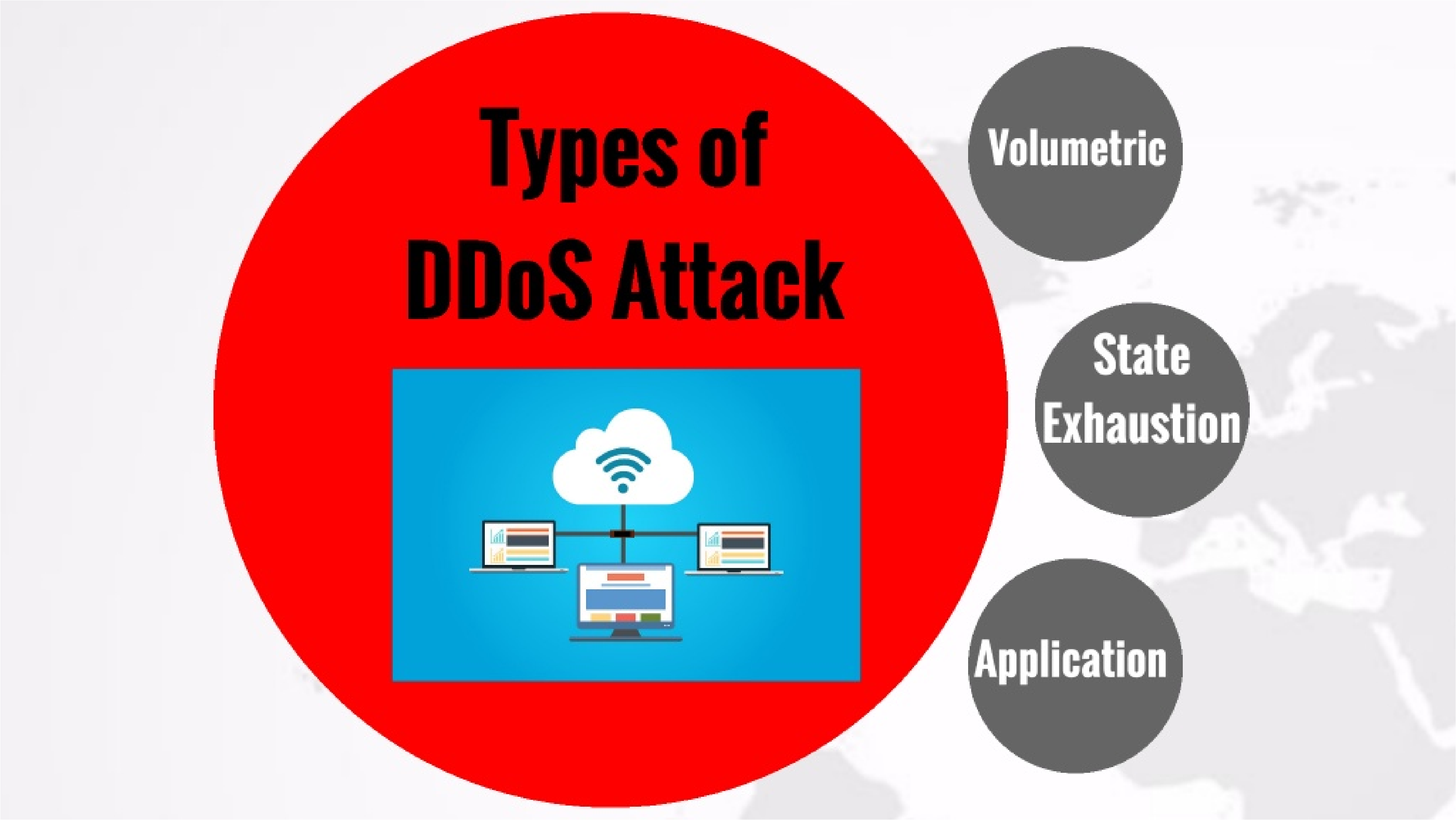

Smurf Attack
Attacker
Victim
ICMP Packets with spoofed IP
ICMP Responses redirected to victim





Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

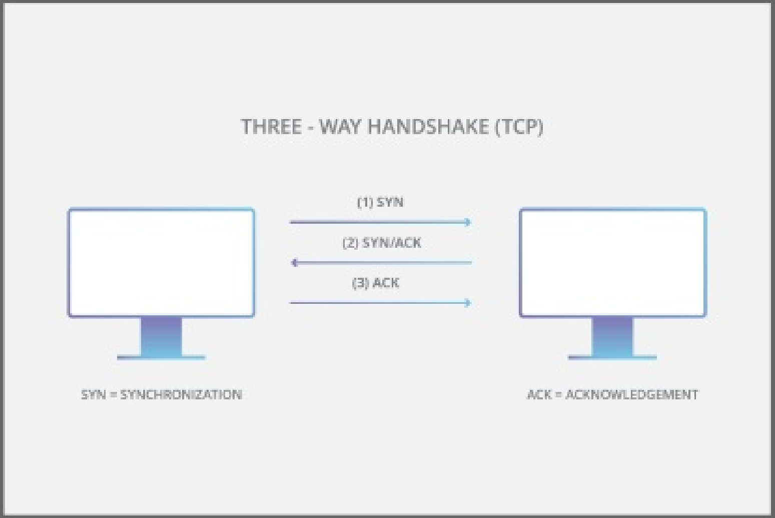


Types of DDoS Attack

- Volumetric
- State Exhaustion
- Application

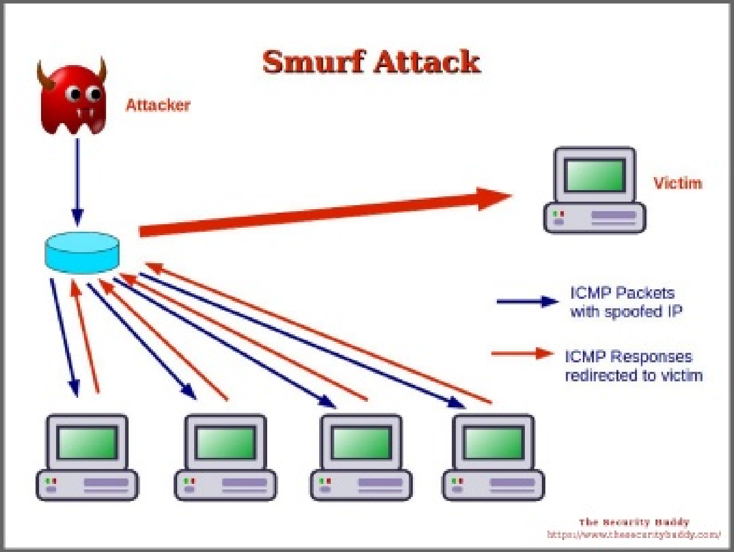
Volumetric

- TCP flood
- ICMP flood
- UDP flood



State-Exhaustion

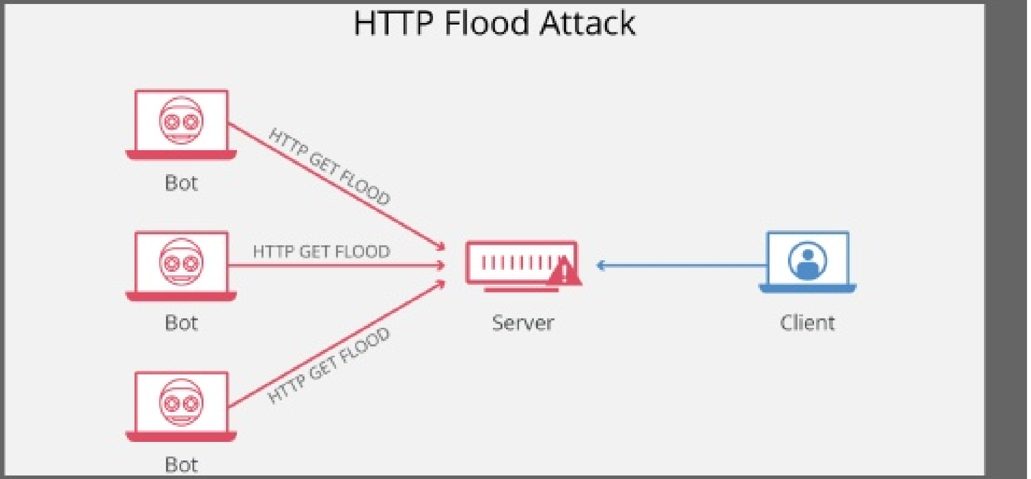
- Smurf Attack
- Ping Flood
- SYN Flood

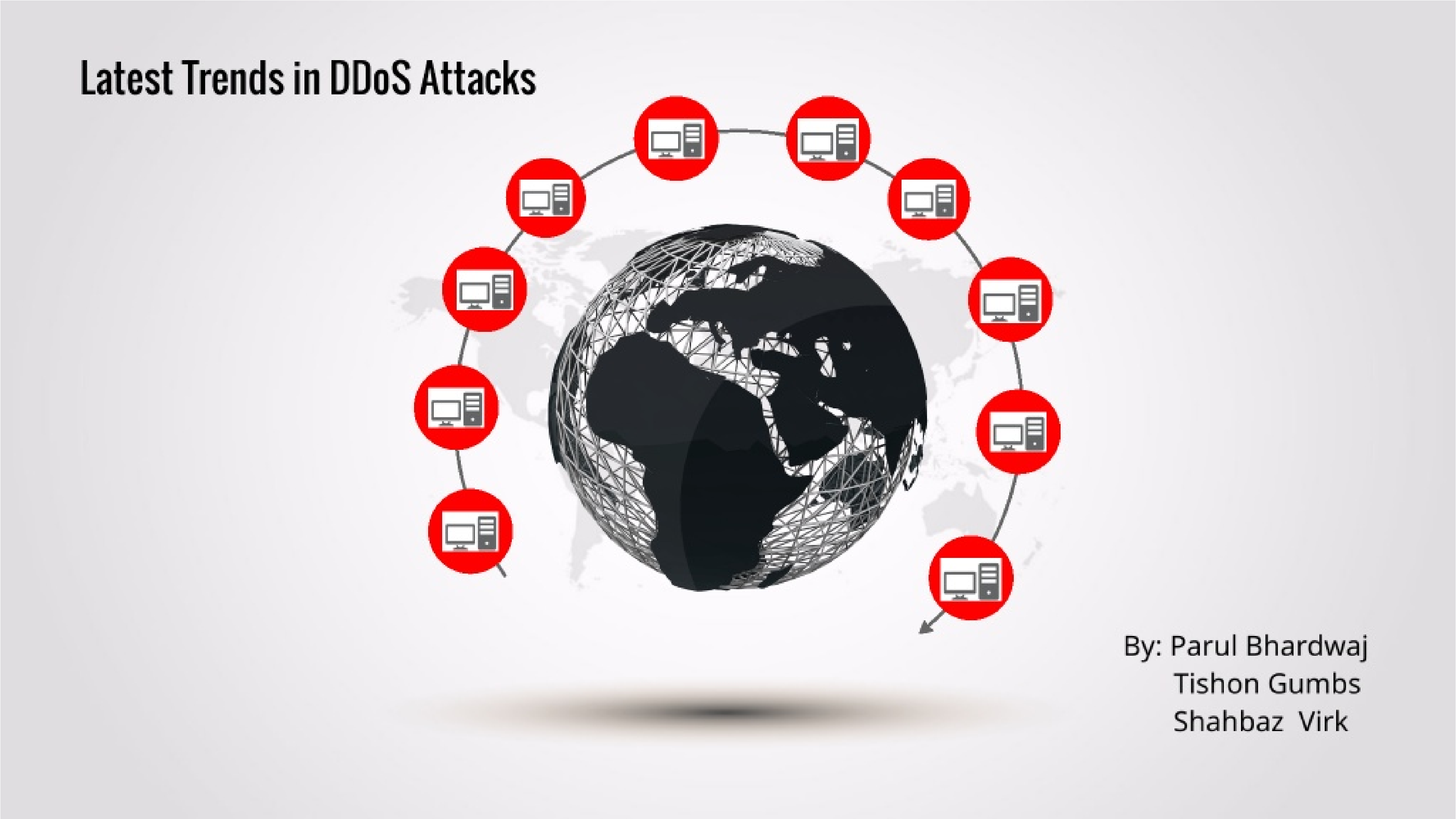

Smurf Attack
Attacker
Victim
ICMP Packets with spoofed IP
ICMP Responses redirected to victim
The Security Buddy
https://www.thesecuritybuddy.com/

Application

- Hash DoS attack

- TearDrop attack





Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

Rise of DDoS Attacks

2013-2014

2015

2016

2017

2018

2013- 2014

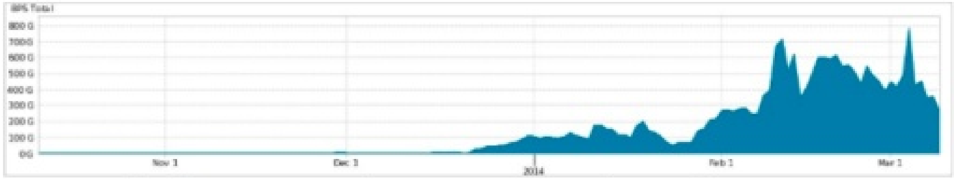
The Time is Now

Network Time Protocol

A series of NTP reflection/amplification attacks were launched against multiple online gaming services, causing widespread outages.

Average NTP traffic globally in November 2013 was 1.29 GB/sec, by February 2014 it was 351.64 GB/sec

NTP was used in 14% of DDos events overall but 56% of events over 10 GB/sec and 84.7% of events over 100 GB/sec

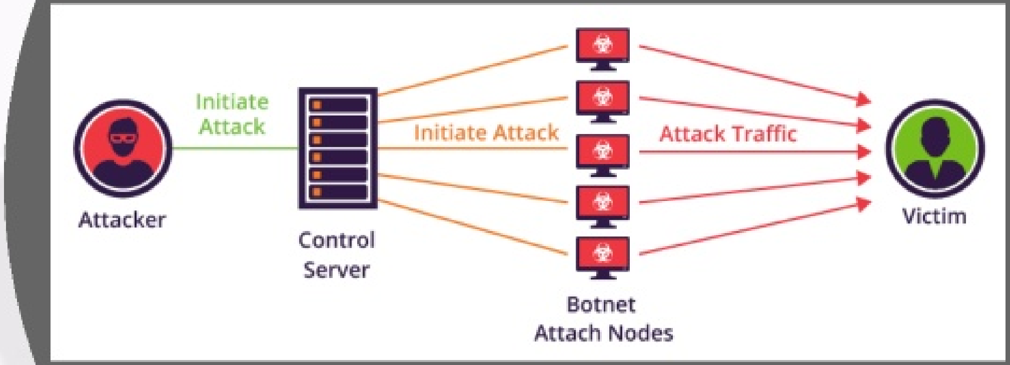


NTP traffic from December 2013 through March 2014

2015

Rise of IOB

By 2015, UDP- based reflection/ amplification attacks were responsible for generating some of the largest volumetric DDoS flood attacks ever observed.



2016

No Stone Unturned

In 2016, ATLAS documented a strong resurgenece of DNS as the dominant protocol being leveraged for reflection/ amplification attacks

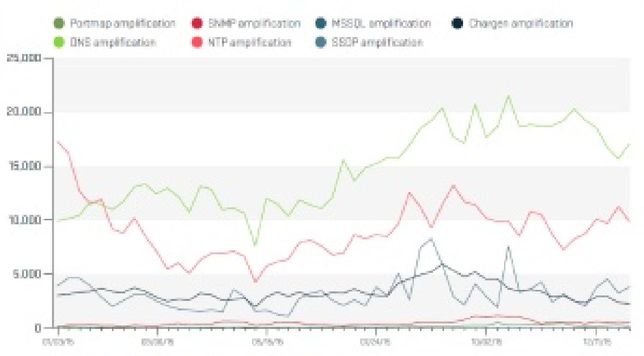


Figure AT10 ATLAS Reflection/Amplification Attacks, Count Per Week

Mirari Botnet

- Mirai is a self-propagating botnet virus
- The Mirari botnet code infects poorly infected devices by using telnet to find those that are still using factory default

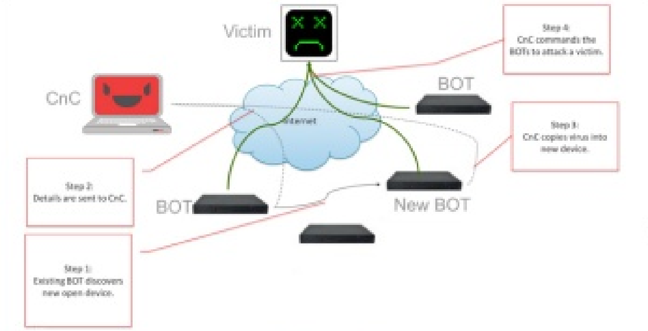
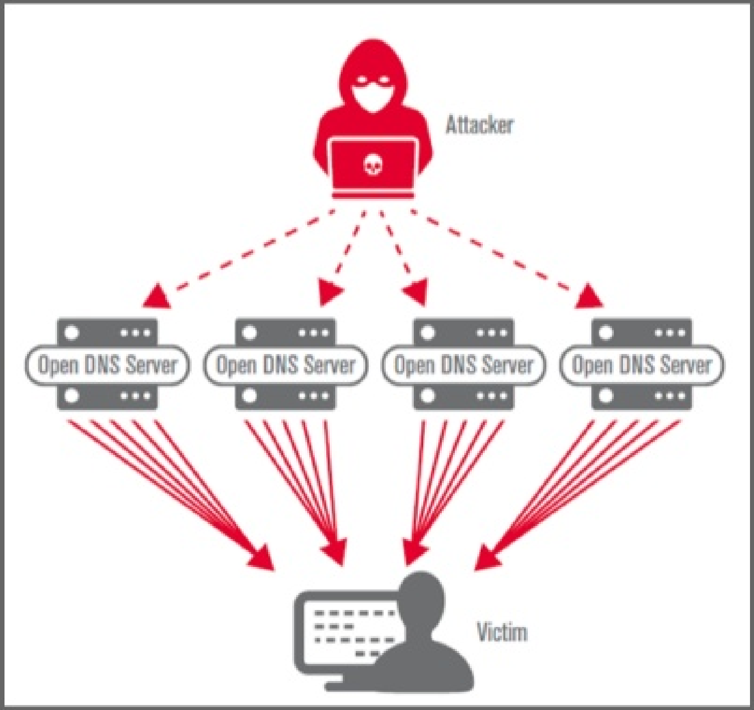

Victim
Step 4:
CnC commands the BOTs to attack a victim.
CnC
BOT
Internet
Step 3:
CnC copies virus into new device.
Step 2:
Details are sent to CnC.
BOT
New BOT
Step 1:
Existing BOT discovers new open device.

Figure 1 Mirai System

2017

Success Breeds Imitation

In 2017, attackers continued to use reflection/ amplification techniques to exploit vunerabilities in DNS, NTP, SSDP, CLDAP, Chargen and other protocols to maximize the scale of their attacks

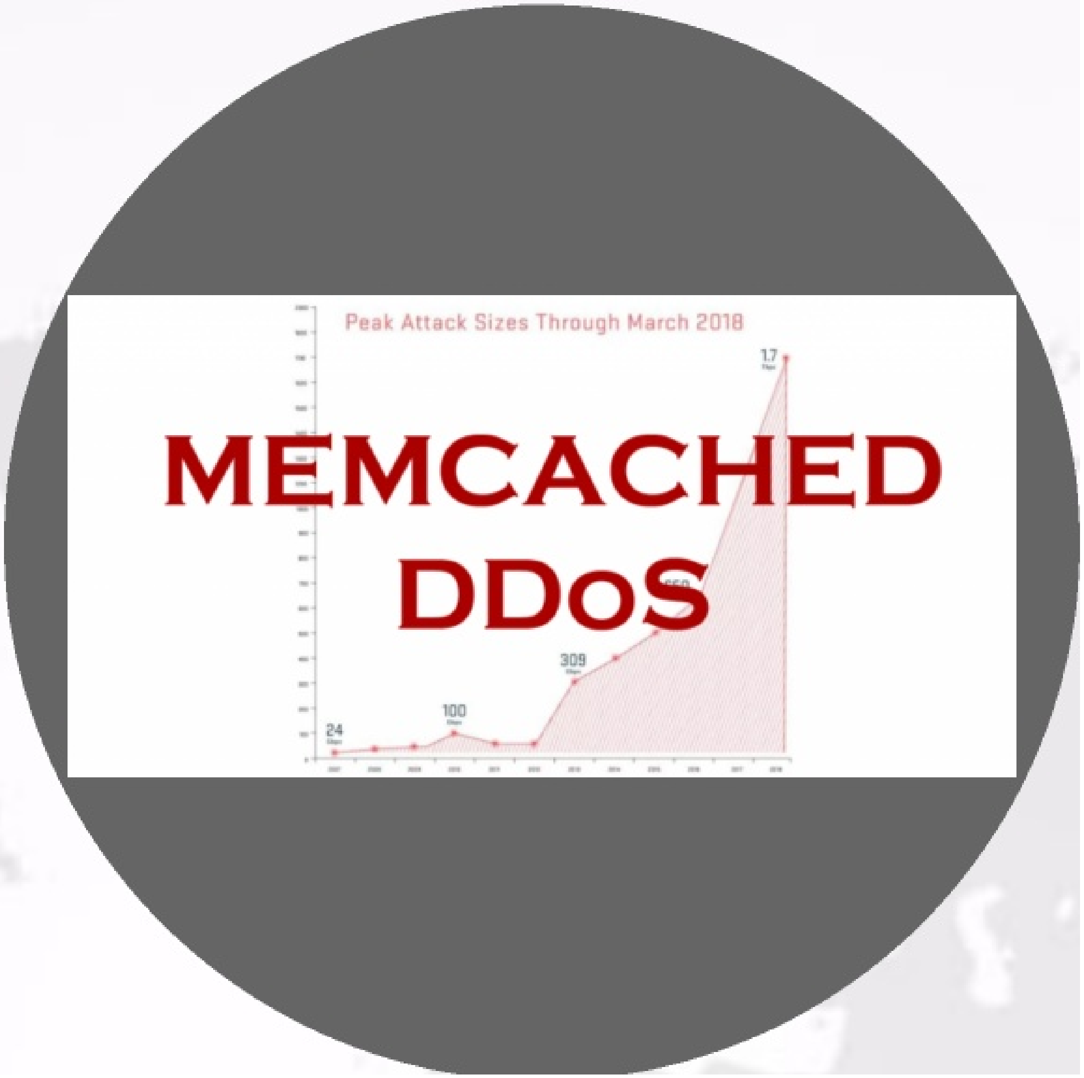


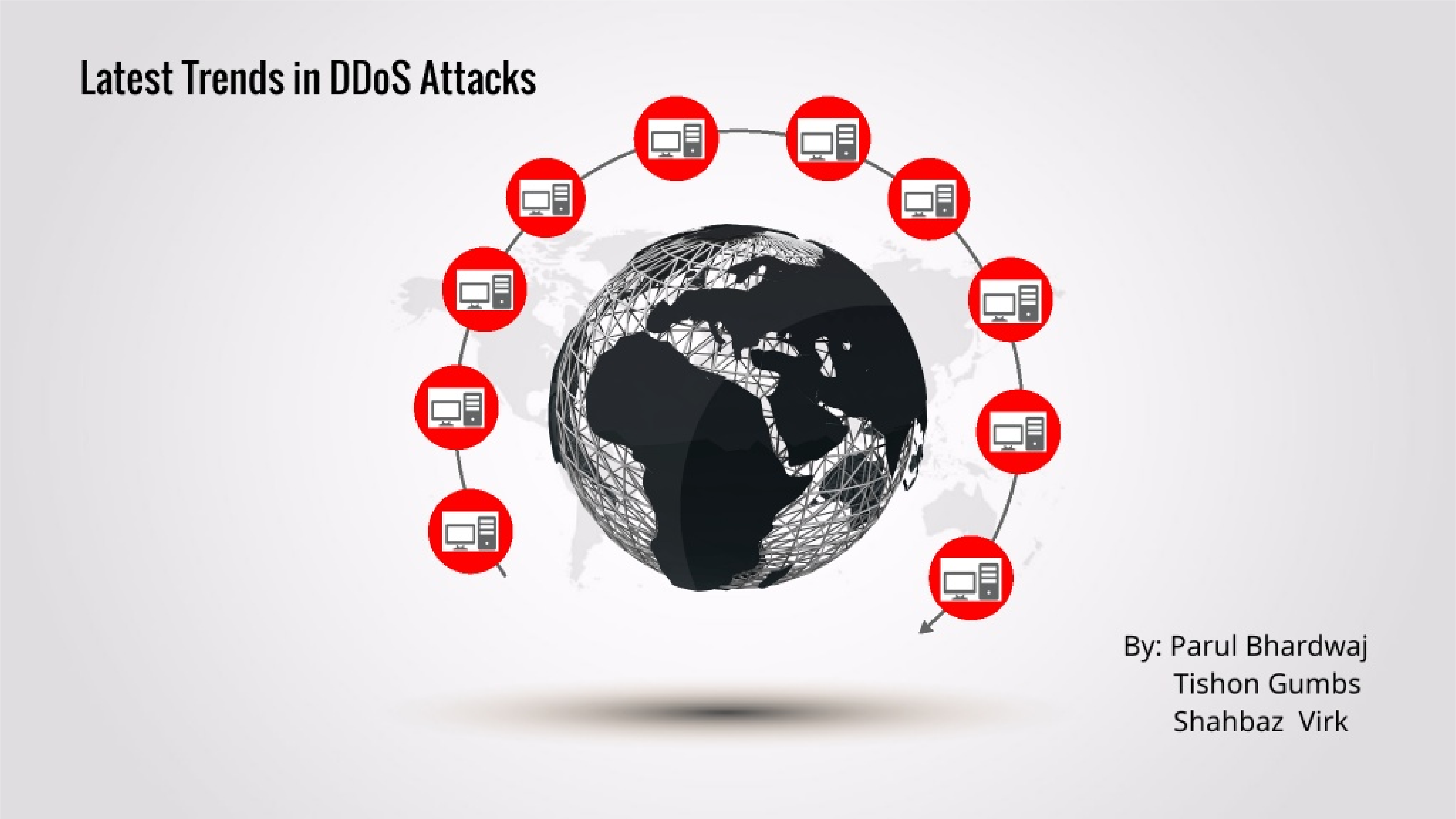
2018

Memcached: High-bandwidth reflection/amplification exploits

In 2018, another widely used application, memcached, has joined the ranks of high-bandwidth reflection/amplification exploits.

Open source and free, memcached is a high-performance, distributed memory caching system designed to optimize dynamic web applications.





Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

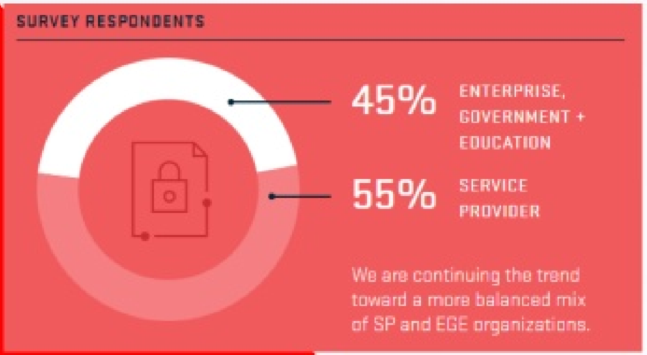
DDoS Attack Key Insights

Targets

Complexity

Noteworthy

Major Targets

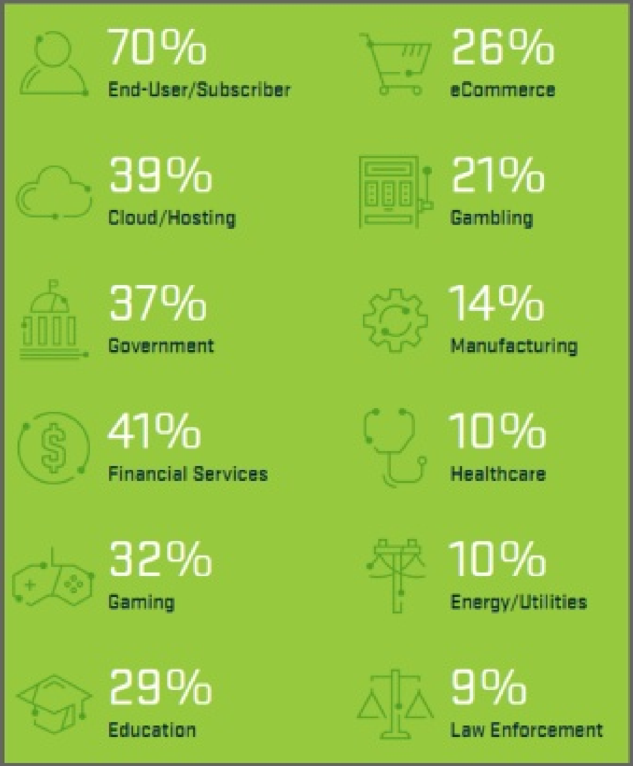


SURVEY RESPONDENTS

45% ENTERPRISE, GOVERNMENT + EDUCATION

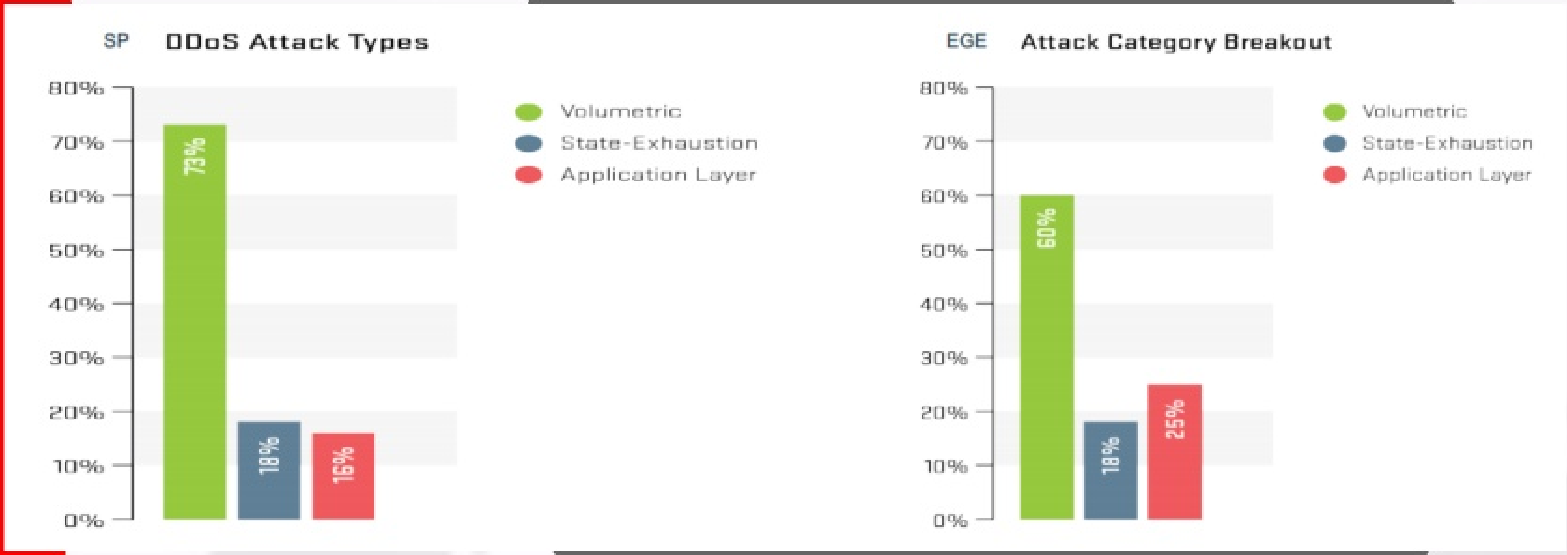
55% SERVICE PROVIDER

We are continuing the trend toward a more balanced mix of SP and EGE organizations.



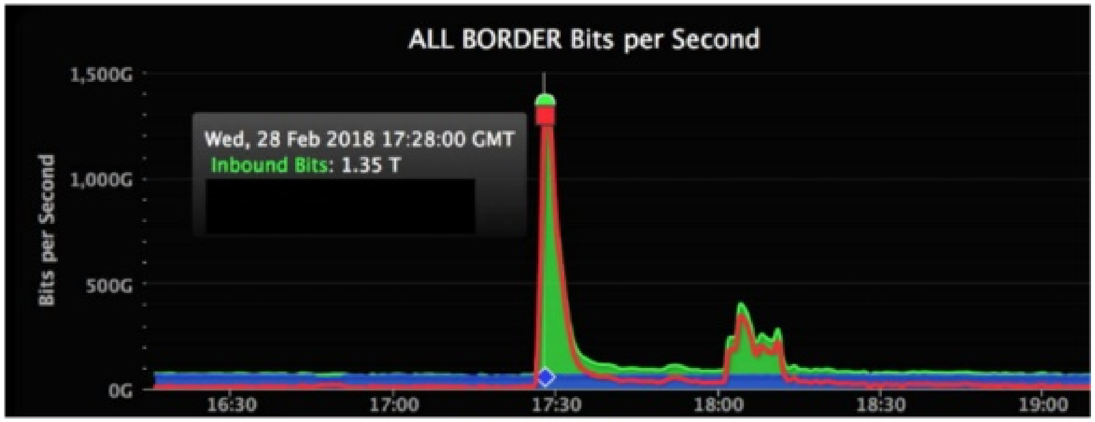
70% End-User/Subscriber	26% eCommerce
39% Cloud/Hosting	21% Gambling
37% Government	14% Manufacturing
41% Financial Services	10% Healthcare
32% Gaming	10% Energy/Utilities
29% Education	9% Law Enforcement

Complexity: Attack Types

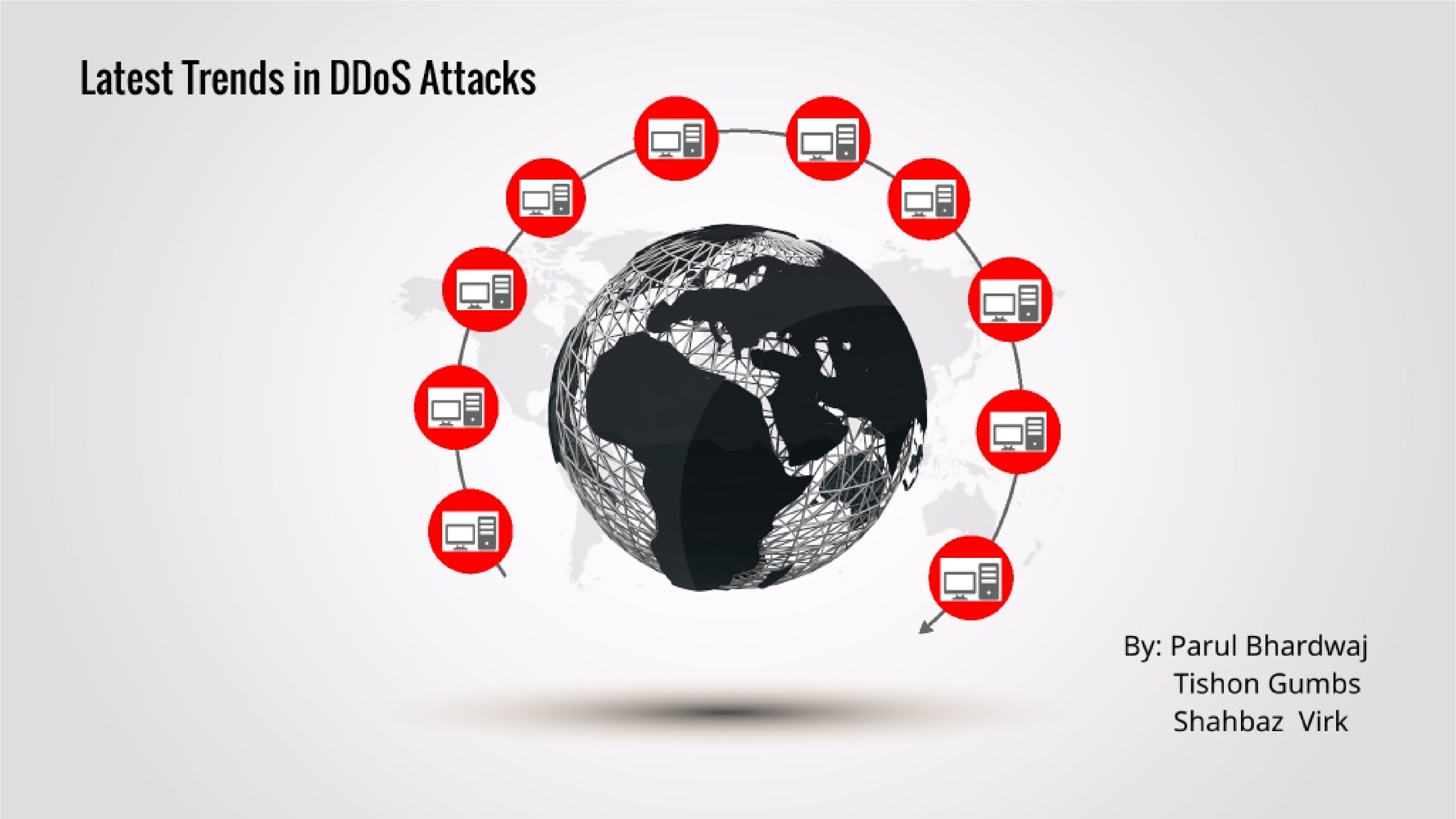


Famous DDoS Attacks

- **Github**: 1.35 TBPS
- **Occupy Central, Hong Kong**: 500 GBPS
- **Cloudfare**: 400 GBPS



GitHub DDoS Attack



Latest Trends in DDoS Attacks

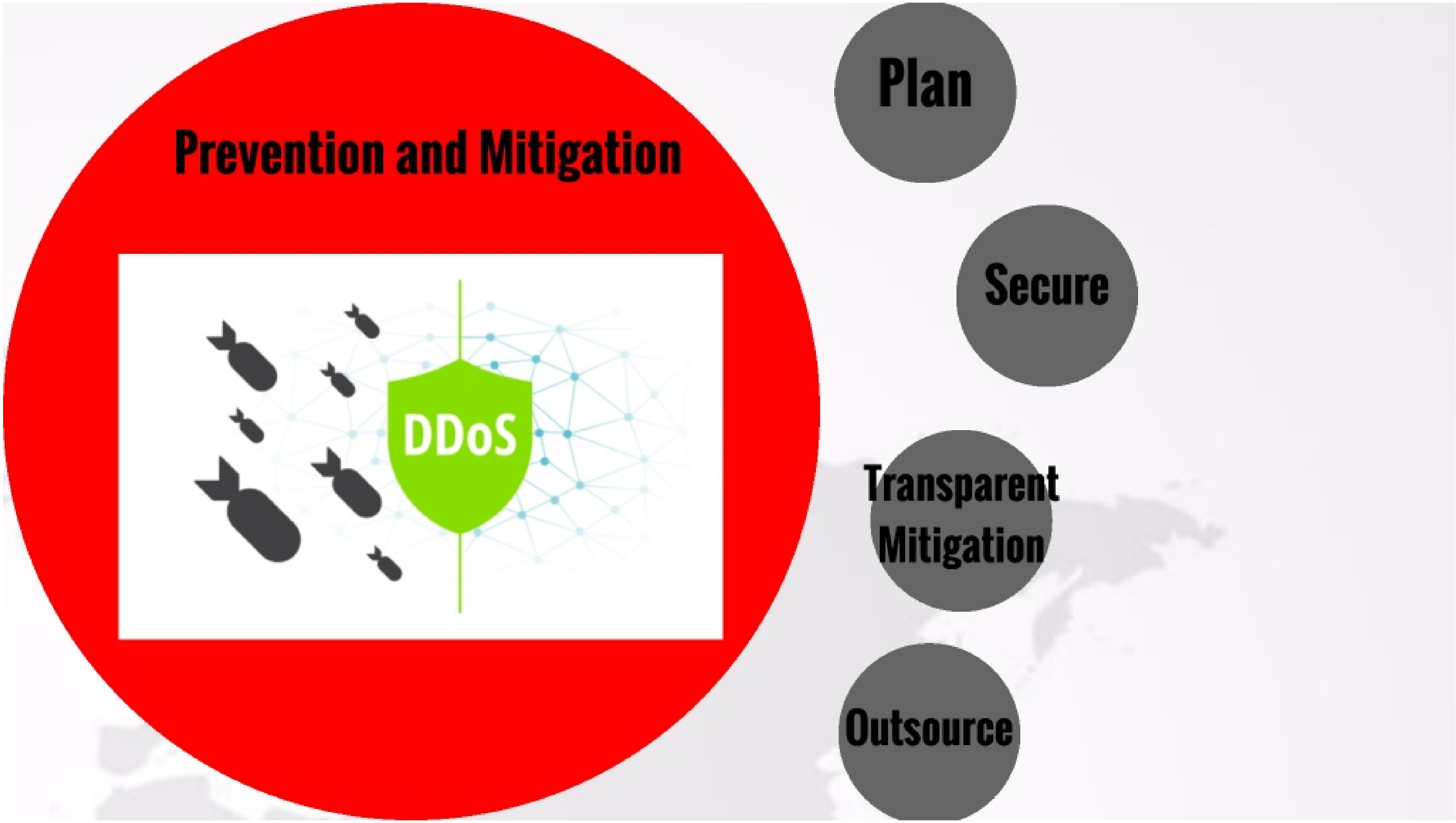
By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

Challenges

- **Rising Threats:** Numerous Stronger attacks
- **Greater Variety:** Different server parts targeted with combinations of several attack strategies
- **Mitigation Gap:** Only ~57% of organizations have a strategy

Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk



Prevention and Mitigation

Plan

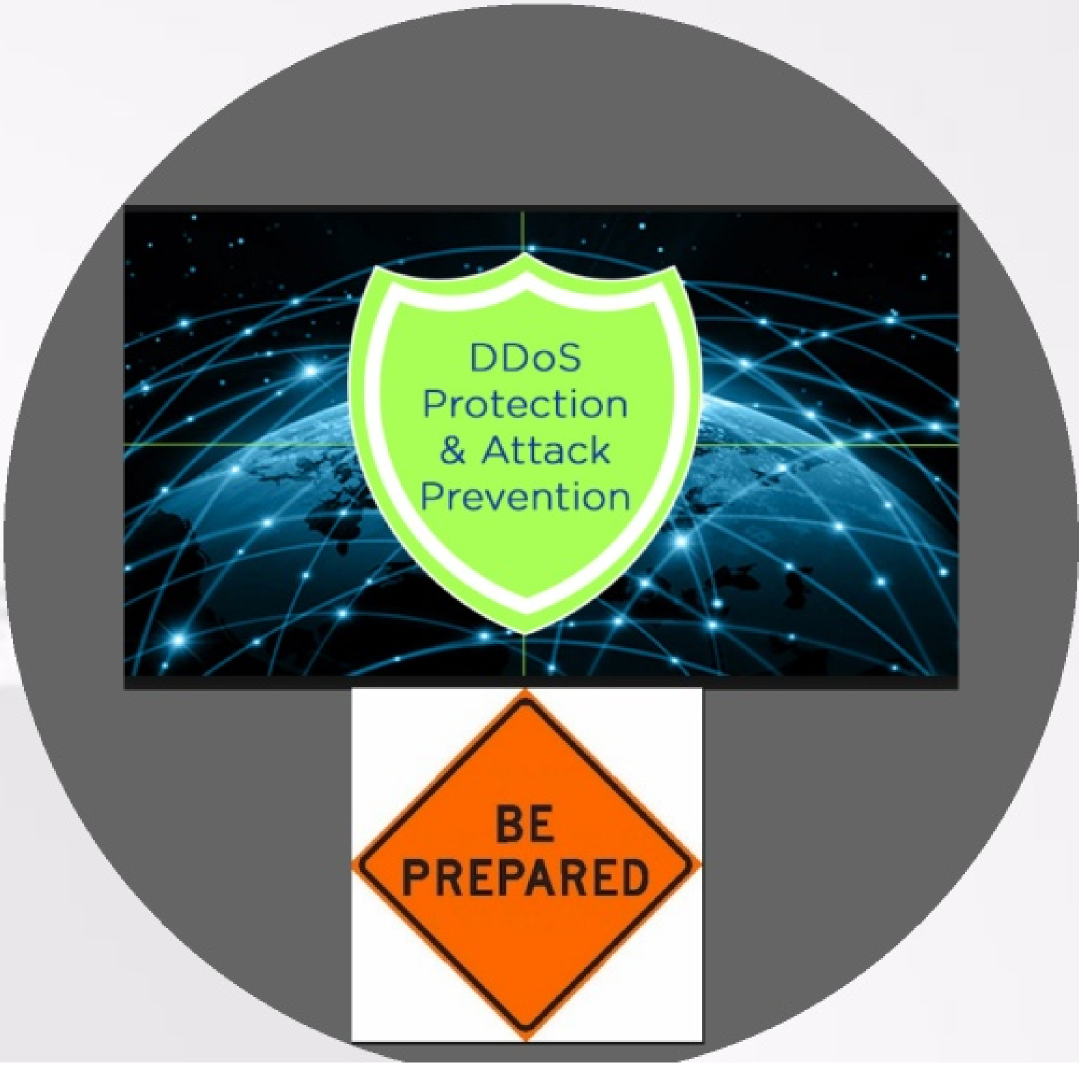
Secure

Transparent Mitigation

Outsource

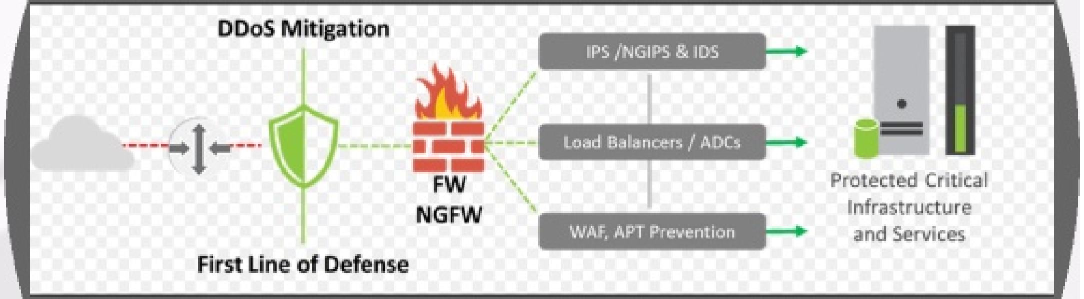
Have a Plan

- Systems Checklist
- Form a response Team
- Define notification and escalation procedures
- Include the list of internal and external contacts



Secure Infrastructure / Network

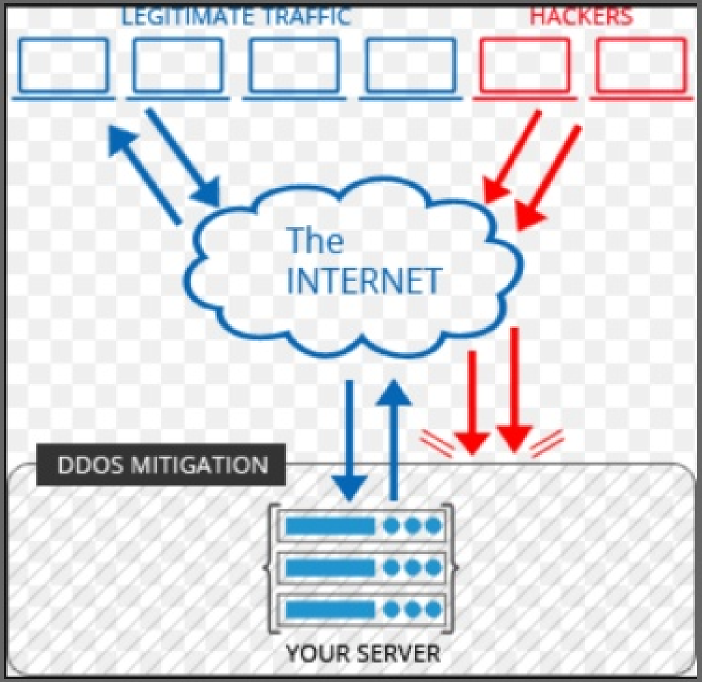
- Firewalls
- VPN
- Anti-spam
- Content-Filtering
- Load Balancing
- Strong Security Practices



Transparent Mitigation

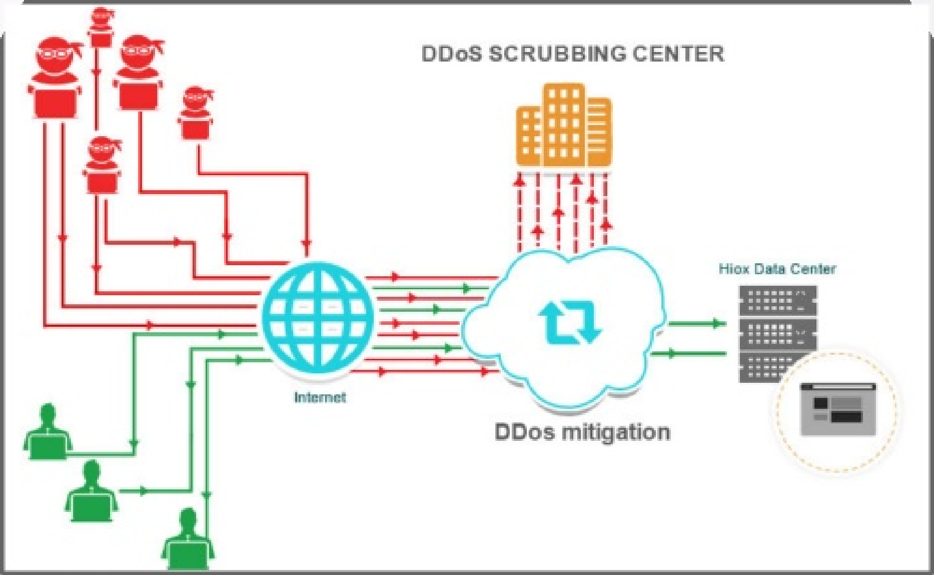
Monitor the Network for:

- Slowdown
- Spotty Connectivity on Intranet
- Intermittent website shutdown
- Incoming/Outgoing Traffic



Outsourcing

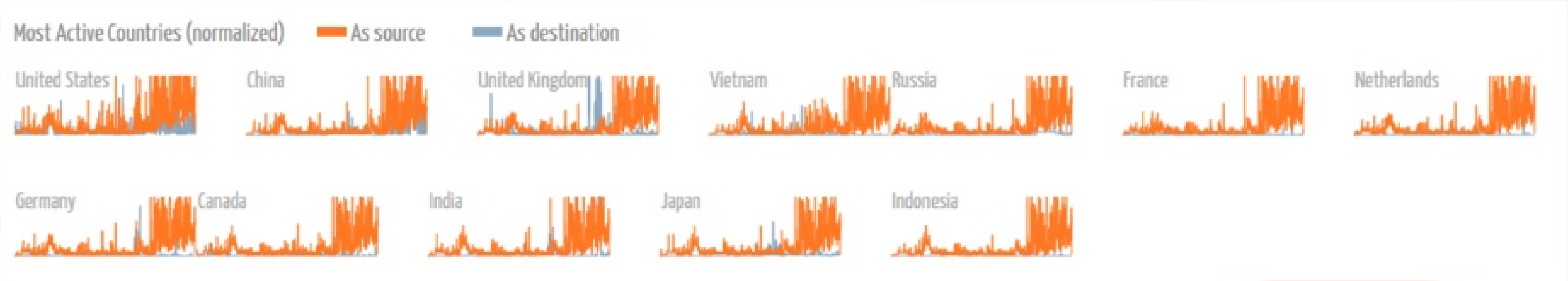
- Leverage the Cloud
- Combination of in-house and third party security service
- Consider DDoS-as -a-Service : Tailor-made security architecture



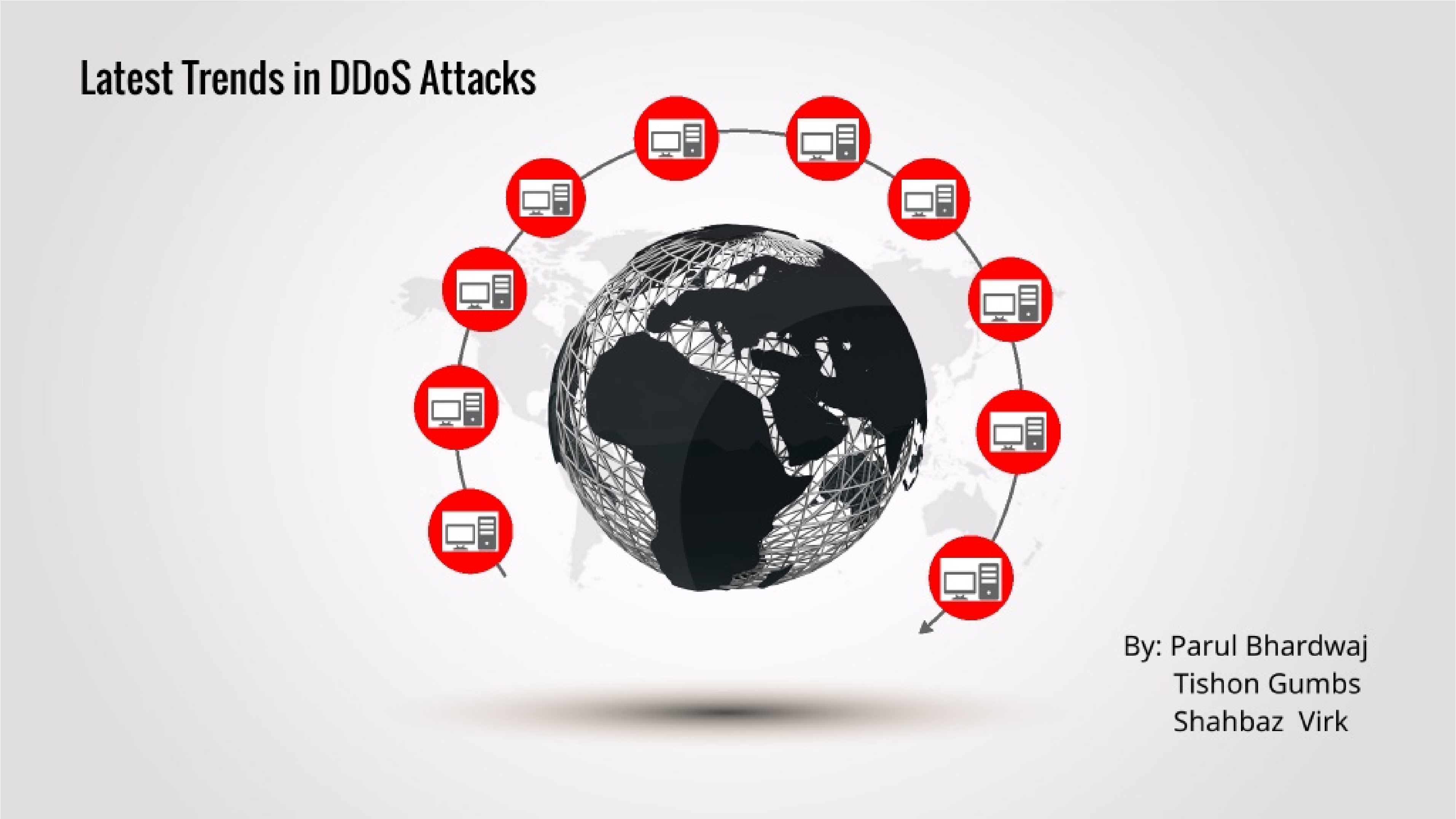
Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

Current DDoS Attack Data



Source: http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17957&view=map



Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

Question time

Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk

References:

+ https://ripe75.ripe.net/presentations/53-RIPE75-DDoS-and-Rise-of-IOT-botnets.pdf

+ https://www.netscout.com/report/

+https://www.nexusguard.com/hubfs/Threat%20Report%20Q2%202018/Nexusguard_DDoS_Threat_Report_Q2_2018_EN.pdf

+ http://info.corero.com/rs/258-JCF-941/images/H1-2018-Corero-Trends-Report-Final.pdf

+https://homes.cs.washington.edu/~arvind/cs425/doc/drdos.pdf

+https://www.colocationamerica.com/blog/preventing-ddos-attacks

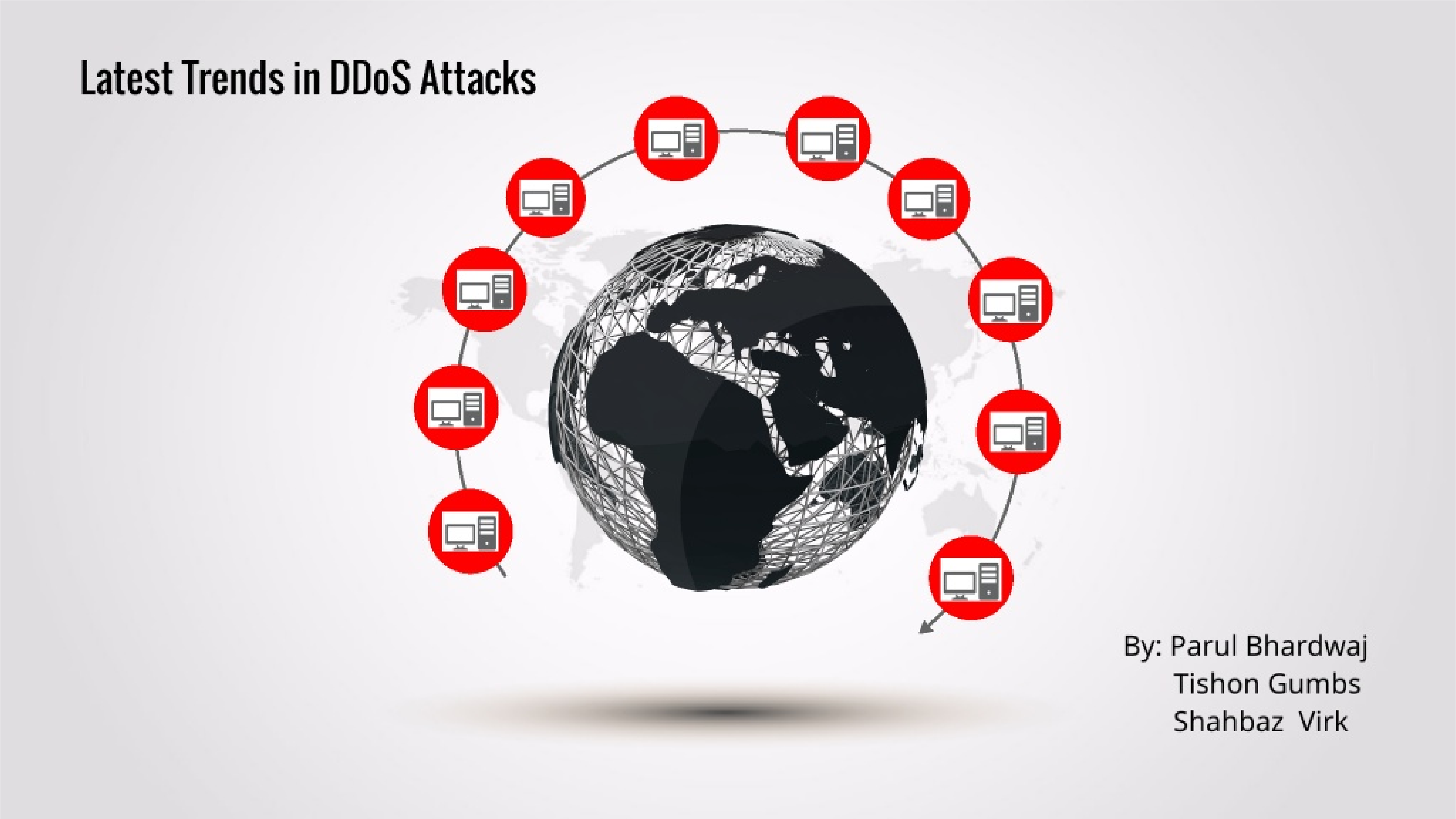
+http://bloggerspath.com/what-is-a-ddos-attack-and-how-to-prevent-it/

+http://www.digitalattackmap.com

+https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html

+https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era

+https://phoenixnap.com/blog/prevent-ddos-attacks



Latest Trends in DDoS Attacks

By: Parul Bhardwaj
Tishon Gumbs
Shahbaz Virk