PURE SECURITY

A TESSERENT COMPANY

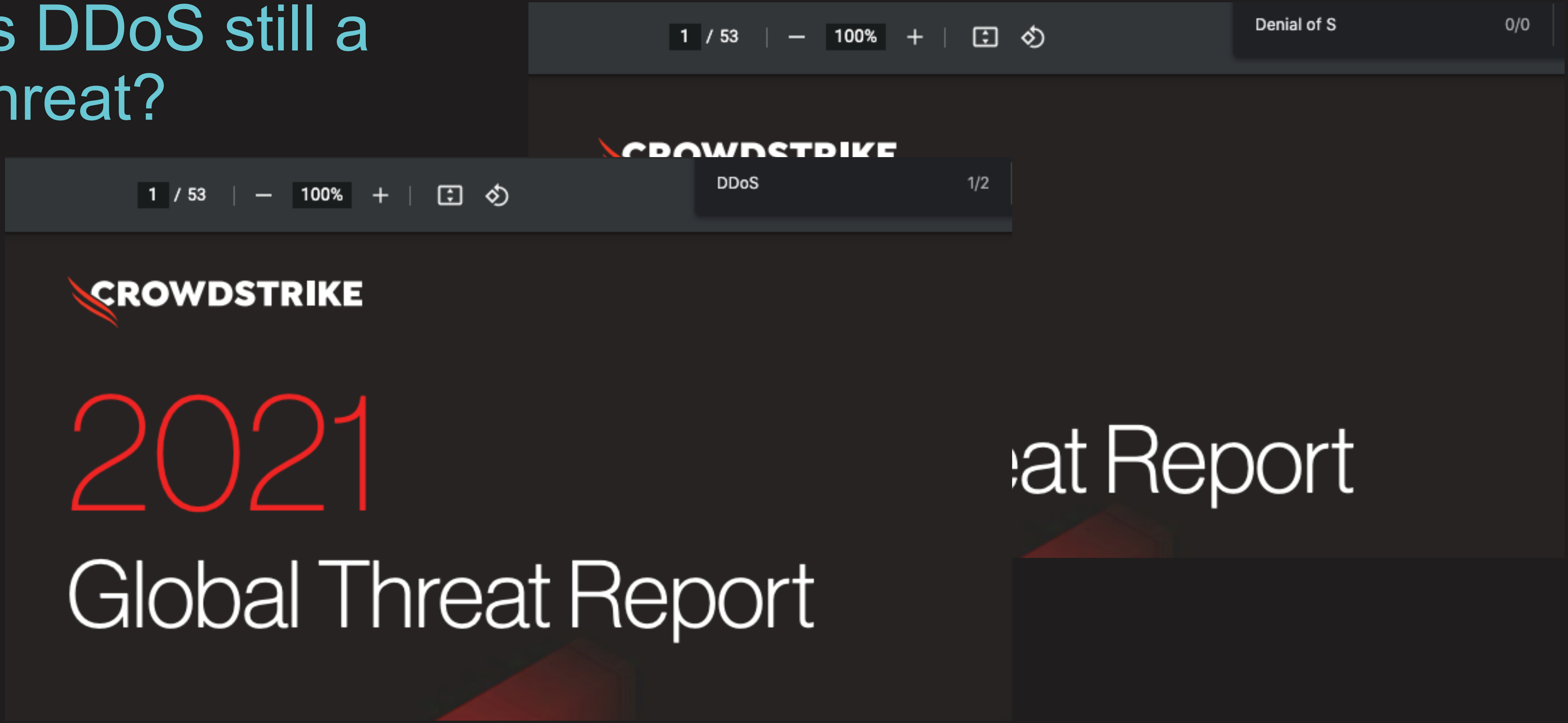
DDoS, is it still a threat?

Arni Hardarson – Head of Assurance

whoami

- Arni Hardarson
- Head of Assurance at Pure Security
  - Running a team of 30 security/offensive consultants
- Been involved in offensive security for the past ~20 years

Is DDoS still a threat?

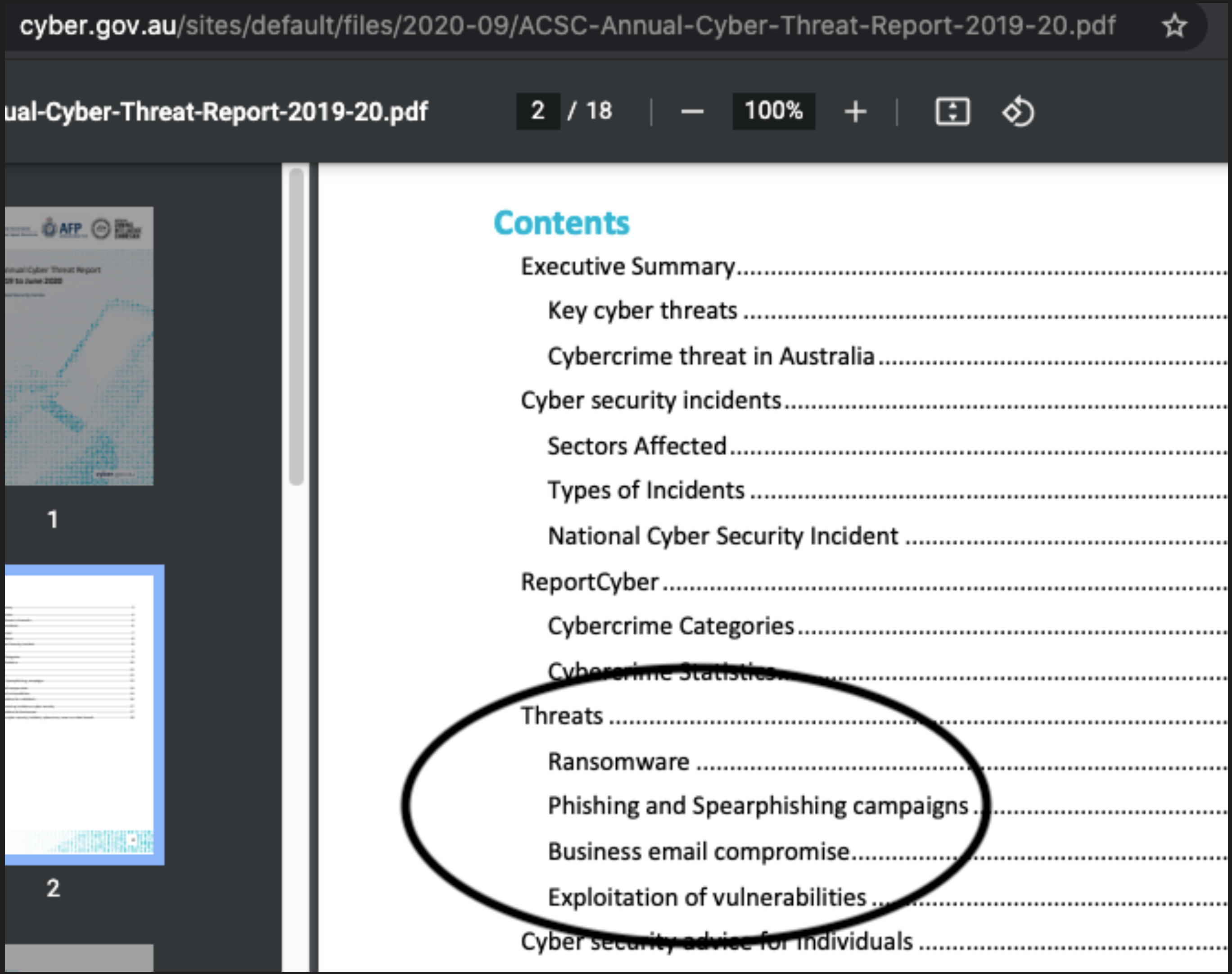


CROWDSTRIKE

2021

Global Threat Report

Is DDoS still a threat?


cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf
ual-Cyber-Threat-Report-2019-20.pdf
2 / 18
100%
1
2

Contents

Is DDoS still a threat?

DDoS attacks dropped by third in Q4 2020 compared to Q3 2020*

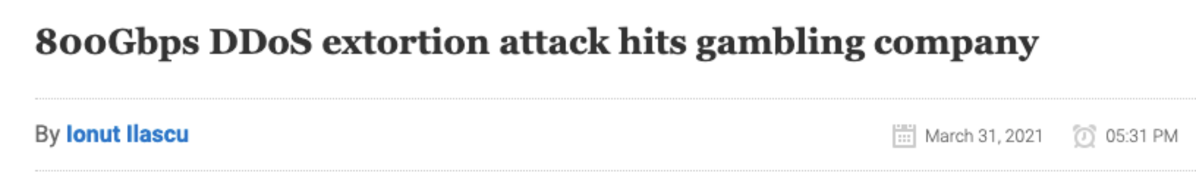
90.72% of DDoS attacks duration period is less than an hour!**

* Kaspersky DDoS Report

** DDoS Attack Trends report from Cloudflare

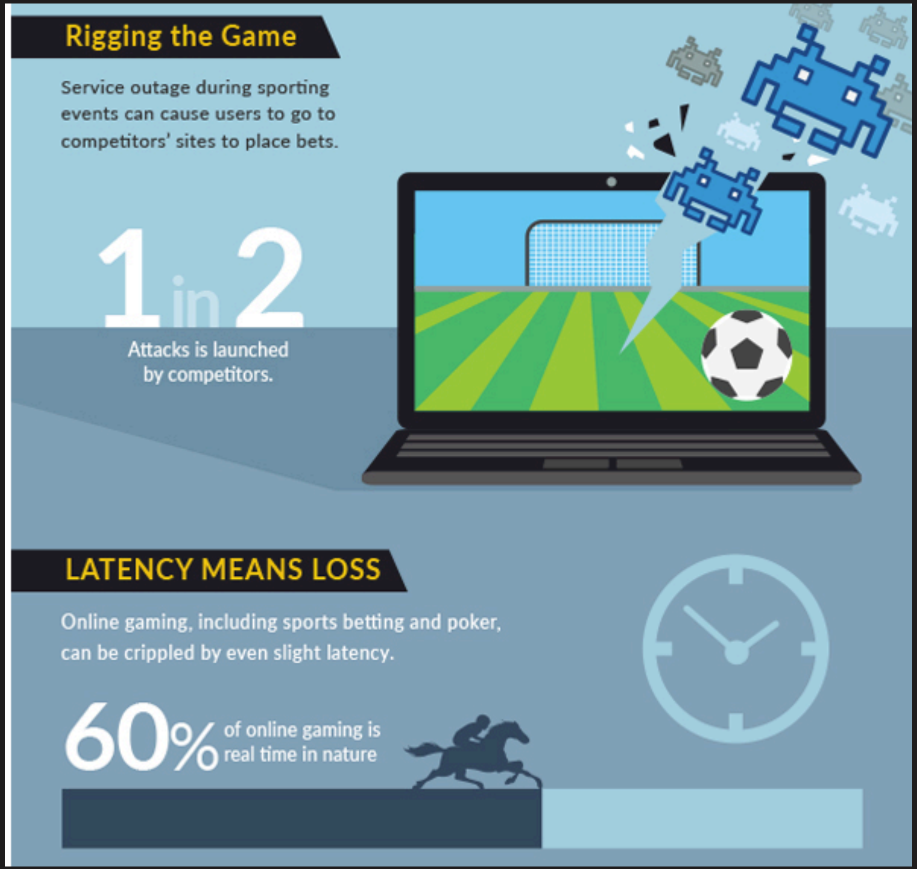
Why is it not considered a major threat for most?

And it’s a major threat for some



800Gbps DDoS extortion attack hits gambling company

By Ionut Ilascu March 31, 2021 05:31 PM



Rigging the Game

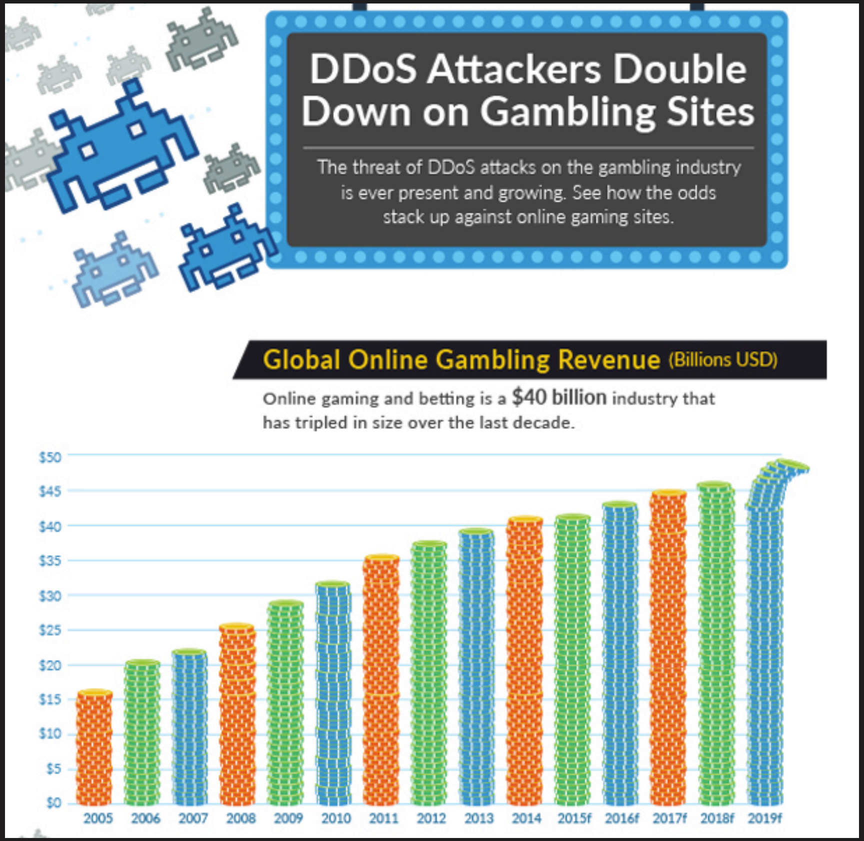
Service outage during sporting events can cause users to go to competitors’ sites to place bets.

1 in 2 Attacks is launched by competitors.

LATENCY MEANS LOSS

Online gaming, including sports betting and poker, can be crippled by even slight latency.

60% of online gaming is real time in nature



DDoS Attackers Double Down on Gambling Sites

The threat of DDoS attacks on the gambling industry is ever present and growing. See how the odds stack up against online gaming sites.

Global Online Gambling Revenue (Billions USD)

Online gaming and betting is a $40 billion industry that has tripled in size over the last decade.

https://www.bleepingcomputer.com/news/security/800gbps-ddos-extortion-attack-hits-gambling-company/

https://www.imperva.com/blog/ddos-attackers-double-down-on-gambling-sites/

How does it work?

- Two types of DDoS attacks
  - Network-layer attacks
  - Application-layer attacks

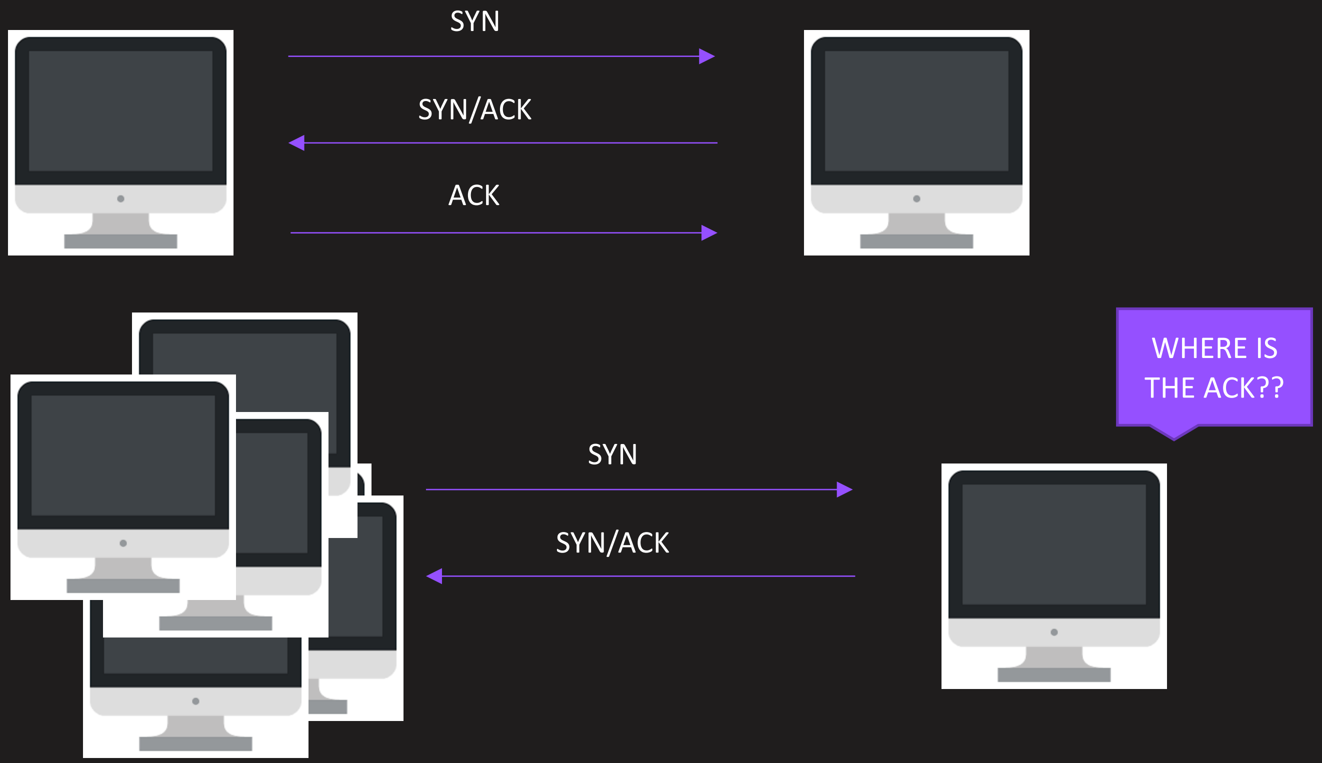
How does it work?

- Network-Layer Attacks
  - DNS Amplification
  - NTP
  - ACK
  - RST
  - SYN
  - SYN-RST-ACK

~63%

How does it work?

- SYN DDoS Attacks
  - Works because it’s exploiting the handshake process of a TCP Connection (3 way handshake)
  - DDoS attack occurs by sending massive amount of spoofed SYN requests to the target server
  - This causes the server to temporarily open a new port while waiting for the last ACK packet
  - As there is a limited number of ports available, once pool is out, server will be unresponsive



How does it work?

- Application-layer Attacks
  - Slowloris
  - Slow Read
  - Slow Post
  - HTTP Flooding (High/Low Orbit Ion Cannon)

How does it work?

- High Orbit Ion Cannon
  - Successor of Low Orbit Ion Cannon
  - Used by Anonymous during the operation Payback campaign
  - Works by flooding the server with HTTP GET and POST requests
  - Successful if it manages to overload the web server request capacity

Emerging threat vector

- Jenkins Servers
  - Jenkins UDP discovery protocol
  - Used to amplify and bounce traffic
  - A single byte request would respond with more than 100 bytes of Jenkins metadata
  - Occurs because of a vulnerability in Jenkins (CVE-2020-2100) and is fixed in v2.219

940% increase this quarter*

Emerging threat vector

Trending technology with browser communication

- Quick UDP Internet Connections (QUIC)
  - General Purpose transport layer protocol designed by Google in 2012
  - More than half of Chrome connection to Google servers are now through QUIC and is support by all major browsers
  - HTTP/3 will use QUIC

- QUIC Reflection DDoS Attack
  - Attackers use this by spoofing the victim’s IP address and by doing so it will result in the server sending all the information to the victim instead of the attacker.
  - Since QUIC utilizes TLS encryption it will result in a simple hello message becoming much larger as the response to the victim includes the TLS certificate as well.

Mitigations

- Deploy a Web Application Firewall (WAF)
- IP Reputation Filtering
- Implement CAPTCHA verification
- Ensure software is up-to-date with patches
- Utilize cloud-based DDoS prevention vendor
  - Manual DDoS mitigation via detection and filtering is not recommended.

Application-layer DDoS Mitigation

Network-layer DDoS Mitigation

Conclusion

- Even though at the moment it is still not a major threat it’s still a threat you should be aware of and ensure you have mitigation in place to protect you.

Takk fyrir

arni.hardarson@pure.security