corero [NETWORK SECURITY]

FRnOG 41

DDoS from SYN-flood to HTTP/3

Ashley Stephenson CTO/CPO v1.2
Corero Network Security

corero [NETWORK SECURITY]

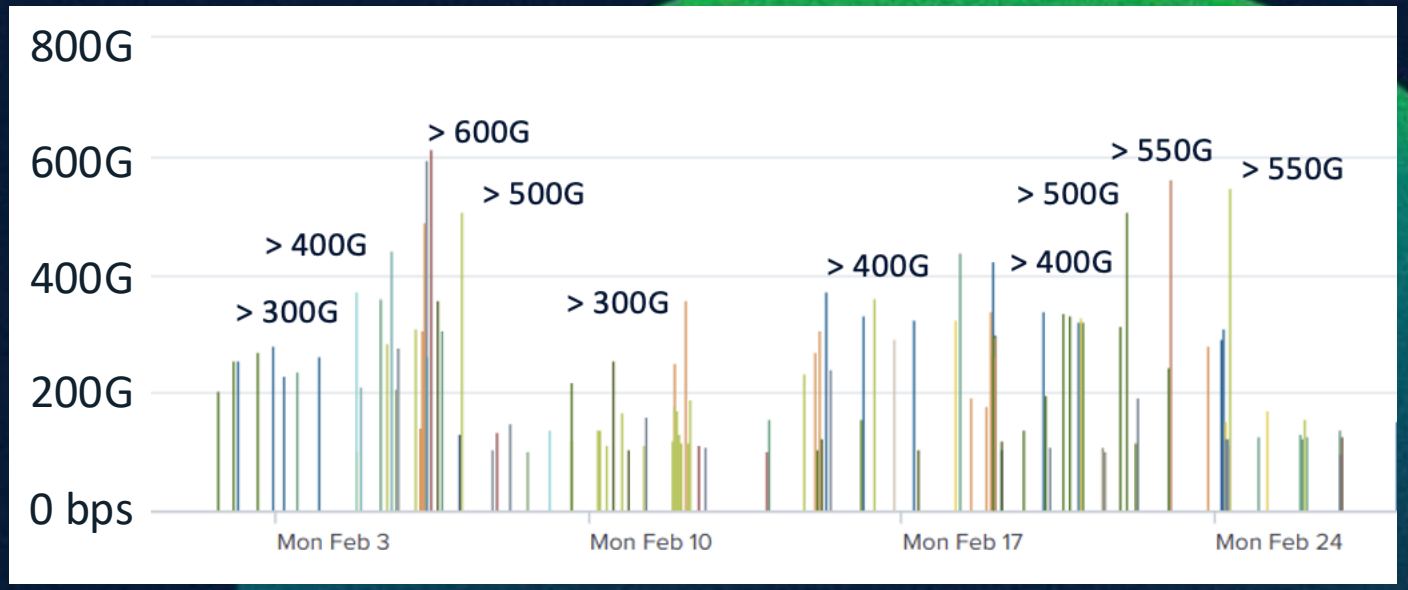
Rule of 10 ?

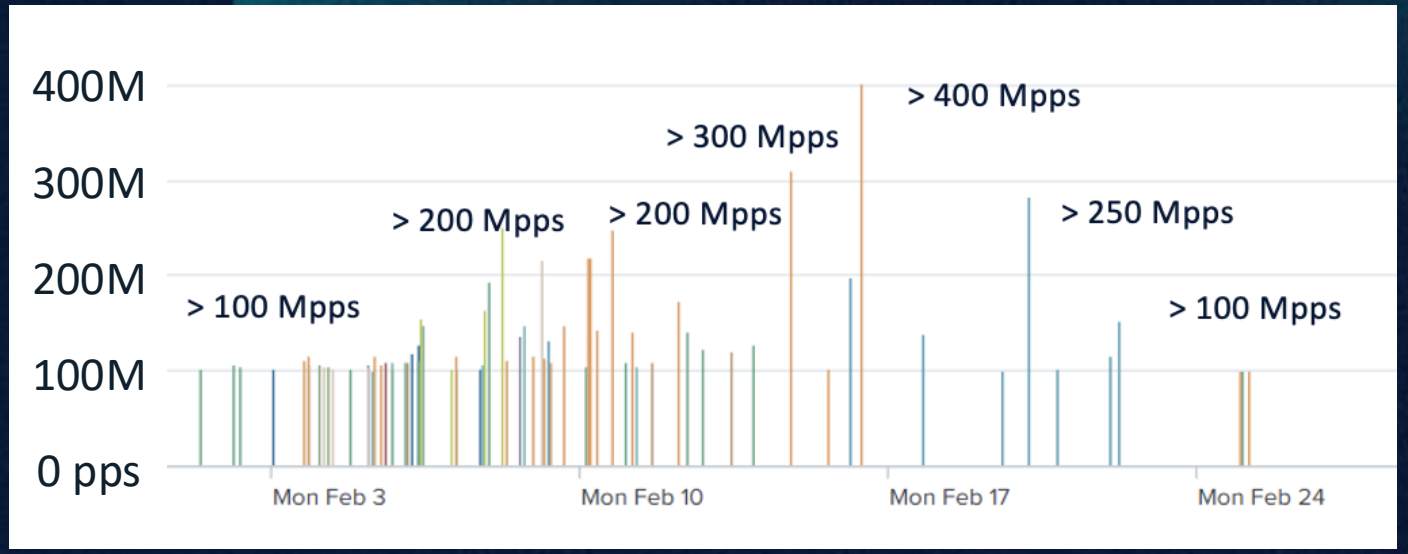
10 Year Trends in DDoS

- From 100G bps to >1T bps
- From 10Mpps to >100Mpps
- 10x number of attacks each 1/10
  - 1Tb -> 100G -> 10G
- 10x number of vectors

…follows Internet Growth

Examples from last month (Feb 2025)





corero [NETWORK SECURITY]

Attack Vectors

Significant growth in the number of attack techniques

- Protocols
- Services
- Bots

Exploits of the **OLD**
Vulnerabilities of the **NEW**

- SYN flood
- Spoofing
- Reflection/Amplification
- Super-amplifiers (Memcached)
- Botnets (Mirai derivatives)
- Tunneled attacks
- Carpet bombing
- DNS water torture (NXdomain)
- Reflections
- L7 exploits
- HTTP/1.1 -> HTTP/2 -> HTTP/3

…follows Internet Evolution

corero [NETWORK SECURITY]

DDoS Modes

- Volumetric (bps)
- Rate (pps)
- Application (cpu/mem/db/$)
- Pulsed (hit-and-run, evasion)
- Sprayed (carpet bomb)
- Multivector
- Other DOS

Resource Exhaustion DDoS
- Connections
- Transaction rate

Ops DoS
- DevOps
- Config Changes
- Security Lockout

PDOS (Permanent)
- Phlashing
- Bricking
- Wiping

Application DDoS
- Query Overload
- Transaction cost
- Botnets

Excuse DDoS
- Deflect Blame
- Cover up Errors

Volumetric DDoS
- Floods
- Reflection/Amplification
- Botnets

Cyber-Kinetic DOS
- Blackouts
- Operational Technology

TDOS
- IP telephony
- Call overload

Self-inflicted DOS
- Config errors
- Software updates
- Bugs

Connectivity DOS
- Broadcast Storms
- Jamming
- Cloning

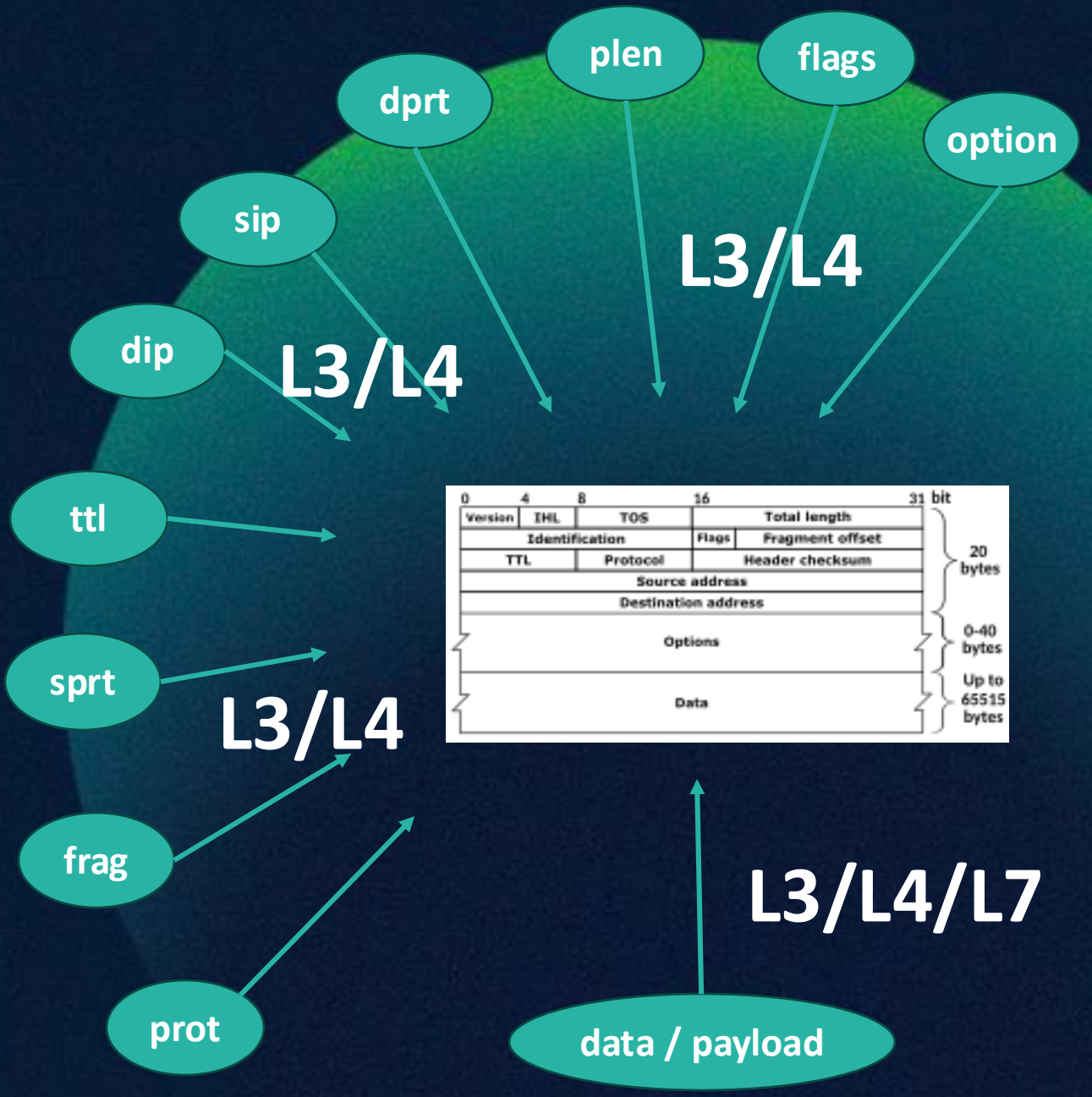
corero [NETWORK SECURITY]

Detecting DDoS

Inspection of Packets

- Counting
- Feature extraction
- Discrimination
- Tracking and Learning
  - (requires state)

all available sources (mirror, sflow, IPFIX, flow, eBPF...)



corero [NETWORK SECURITY]

HTTP/3 Adoption

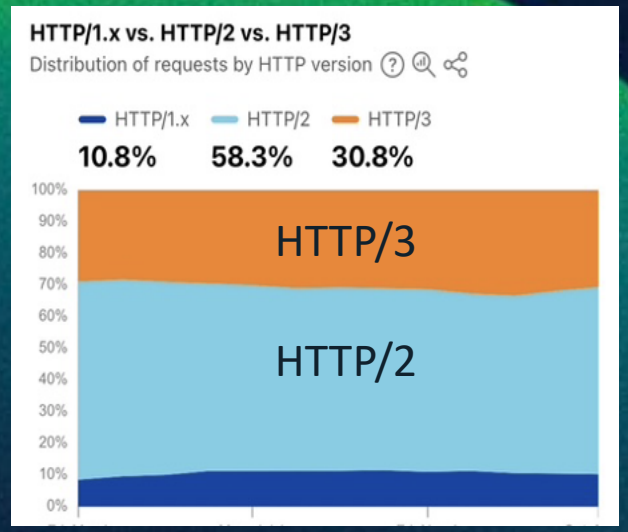
Approx 30% sites using HTTP/3

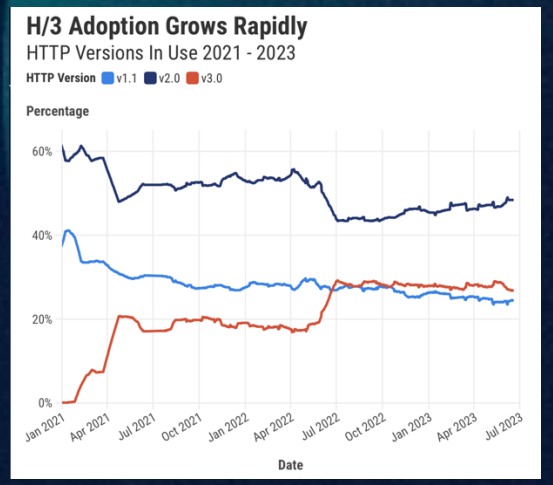
- Browsers (UX) are leading adopters
- M2M are laggards (latency not priority)
- Legacy/IoT devices still using HTTP/1.x

…follows Internet Evolution

Popular sites using HTTP/3

- Google.com
- Facebook.com
- Youtube.com
- Instagram.com
- Linkedin.com
- Cloudflare.com
- Amazon.com
- Bing.com
- Wordpress.org
- Pinterest.com





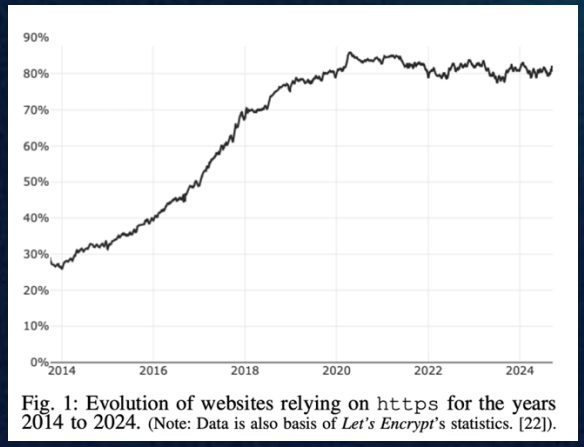


Fig. 1: Evolution of websites relying on `https` for the years 2014 to 2024. (Note: Data is also basis of *Let's Encrypt*'s statistics. [22]).

Source Internet Society, Cloudflare, Mozilla

corero [NETWORK SECURITY]

HTTP/3 and DDoS

Several traditional DDoS techniques translate to HTTP/3

- QUIC Reflections (e.g. spoofed Hello)
- QUIC Floods (e.g. bots - non spoofed)
- We lose the TCP handshake “validation”
- UDP traditionally carries a lot of DDoS
- HTTP/3 always encrypted – challenge!

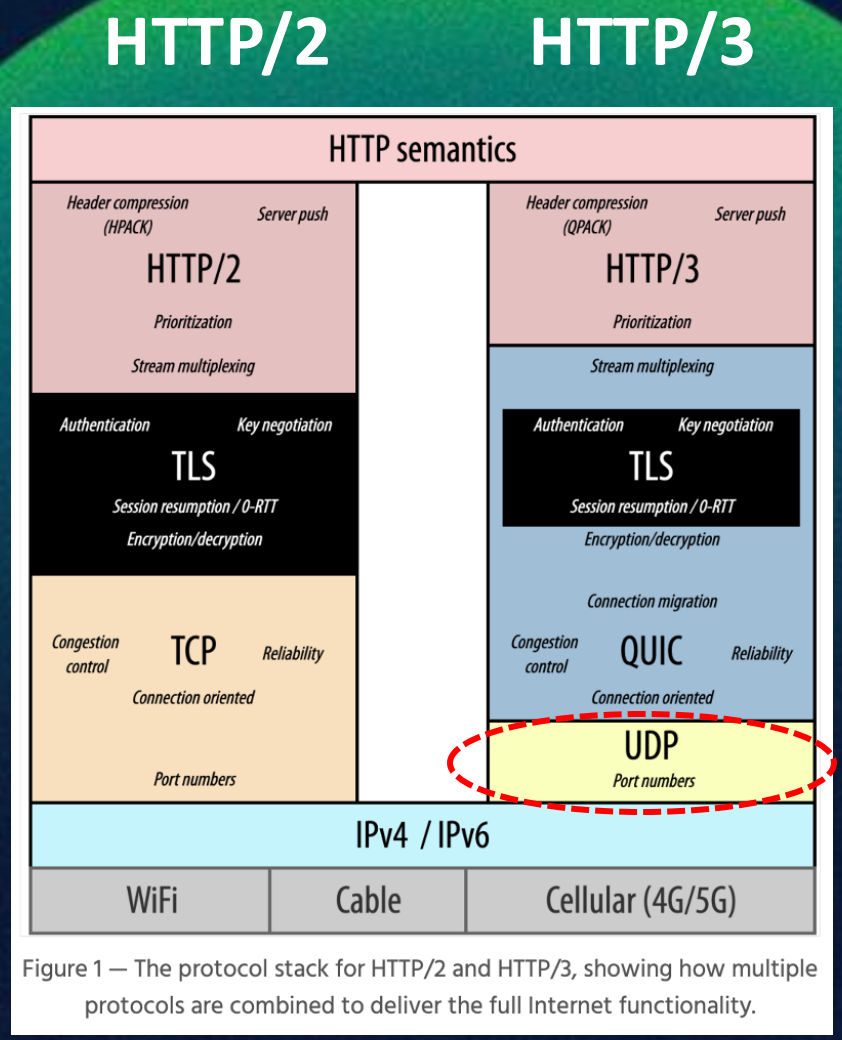


Figure 1 — The protocol stack for HTTP/2 and HTTP/3, showing how multiple protocols are combined to deliver the full Internet functionality.

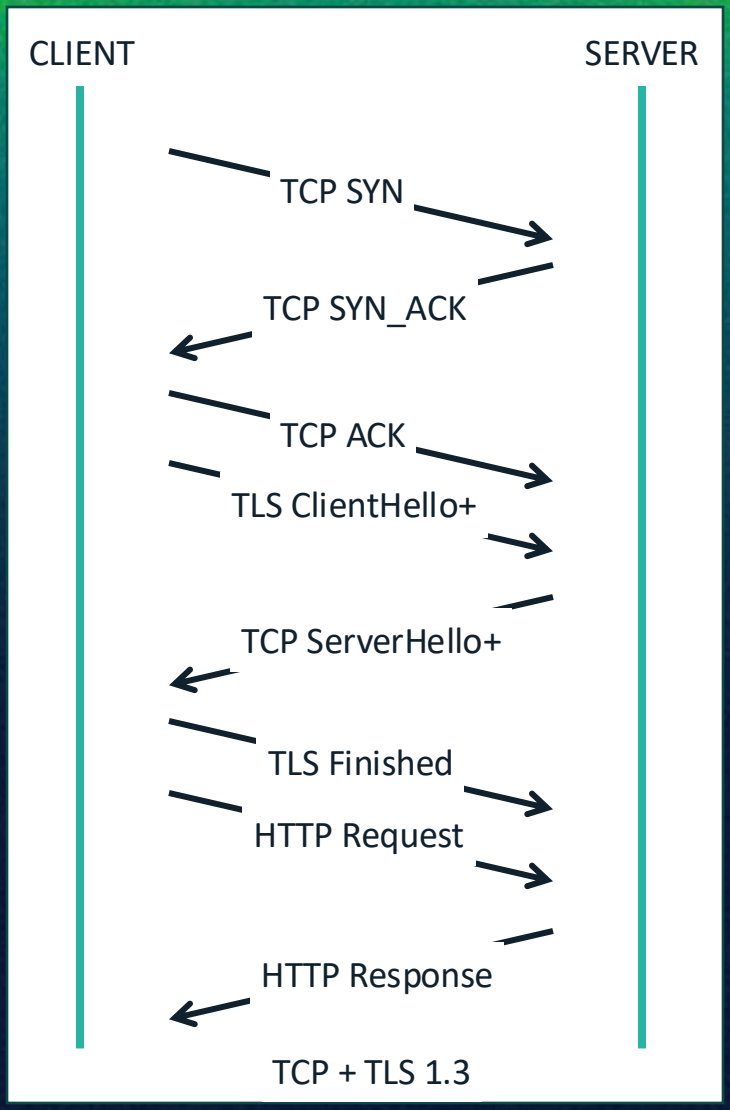
Source:Internet Society

corero [NETWORK SECURITY]

HTTP/2 + TLS + TCP

TCP handshake non-encrypted

- Useful for DDoS inspection
- Well understood, cannot be spoofed
- Helpful for DDoS characterization

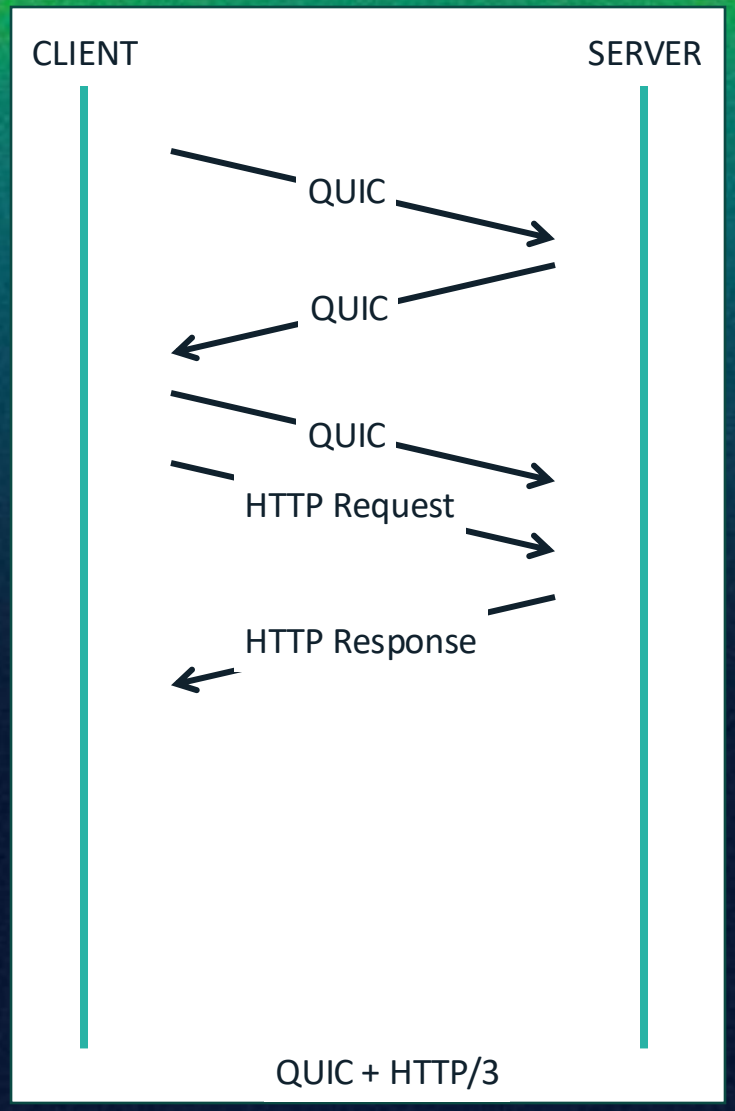


corero [NETWORK SECURITY]

QUIC + HTTP/3

QUIC handshake via datagrams

- **Mandatory use of encryption (TLS 1.3)**
- **Very compact delivery of resource consuming requests**
  - Potential for DDoS Exploitation

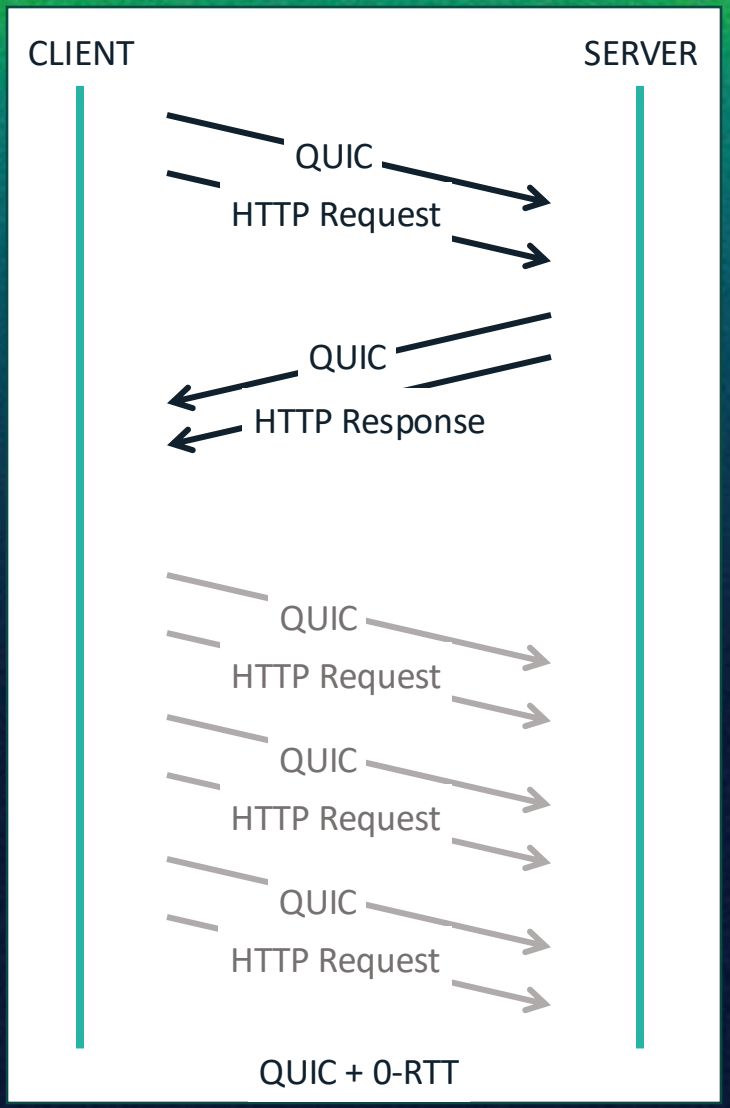


corero [NETWORK SECURITY]

QUIC + 0-RTT

A further optimization

- **Relies on shared secret**
- **Sender can bundle HTTP request with hello**
- **Considered less secure**
  - Vulnerable to replay
  - Potential DDoS exploitation

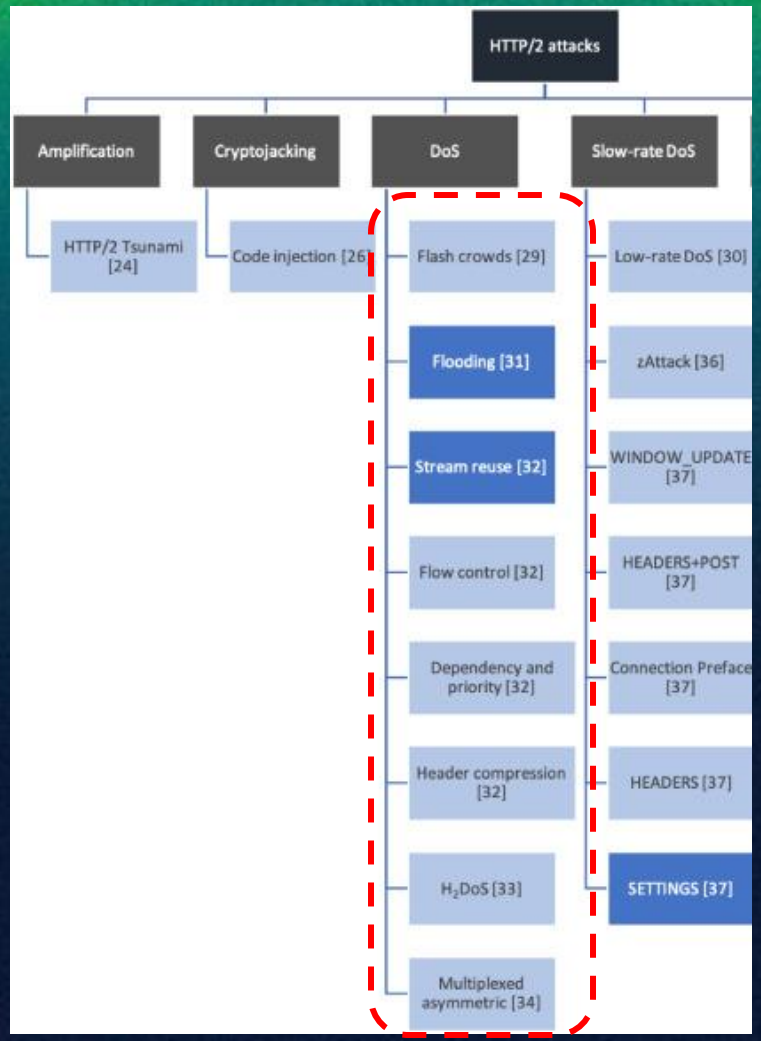


corero [NETWORK SECURITY]

HTTP/3 and DDoS

HTTP/3 is more robust against DDoS exploits than HTTP/2

- **Compare**
  - HTTP/2 DDoS exploits light blue
    HTTP/3 DDoS exploits dark blue
- **Flooding and Stream Reuse persist**
- **New exploits may/will be discovered…**



Source https://www.sciencedirect.com/science/article/pii/S0167404822004436

corero [NETWORK SECURITY]

The Battle Goes On

HTTP/3 is here to stay

- UDP use will continue to increase
- New techniques for DDoS detection and mitigation are being developed
- Network identity (reputation) increasingly important to secure availability

THANK YOU

CORERO.COM

ashley.stephenson@corero.com
patrick.dravet@corero.com