Path Network presentation

RONOG 2022

“DDoS attacks in COVID times”

Virgil Truica

DDoS Security Advocate

✉ virgil@path.net

☎ +40741730735

in linkedin.com/in/virgiltruica

@virgil_T

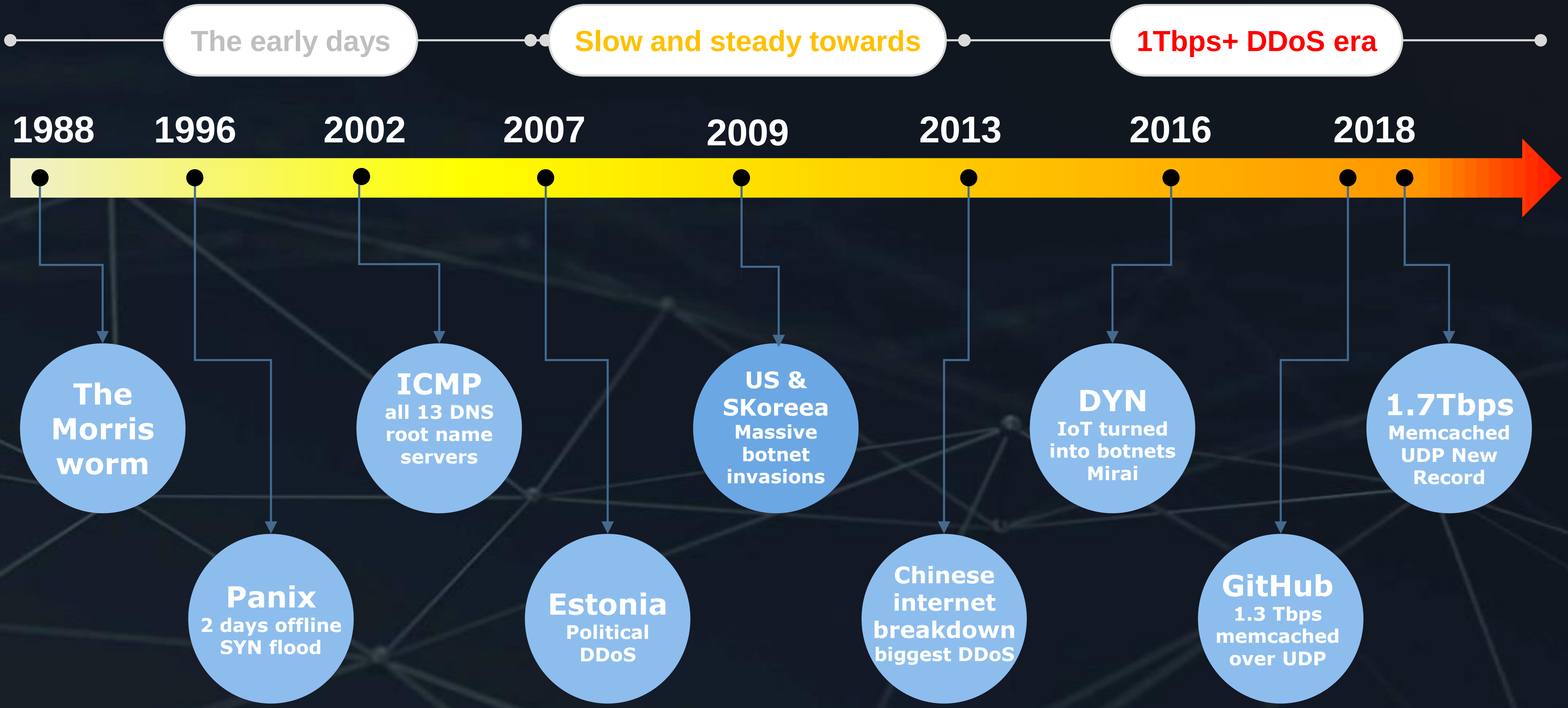
PATH

Agenda

- DDoS Attacks timeline before Covid19
- Covid19 impact on Telecom
- 2019-2022 DDoS stats and facts
- DDoS trends / predictions
- DDoS as a business
- Anti-DDoS solutions available

PATH

DDoS attacks timeline before covid



The early days

Slow and steady towards

1Tbps+ DDoS era

1988 – The Morris worm

1996 – Panix 2 days offline SYN flood

2002 – ICMP all 13 DNS root name servers

2007 – Estonia Political DDoS

2009 – US & SKoreea Massive botnet invasions

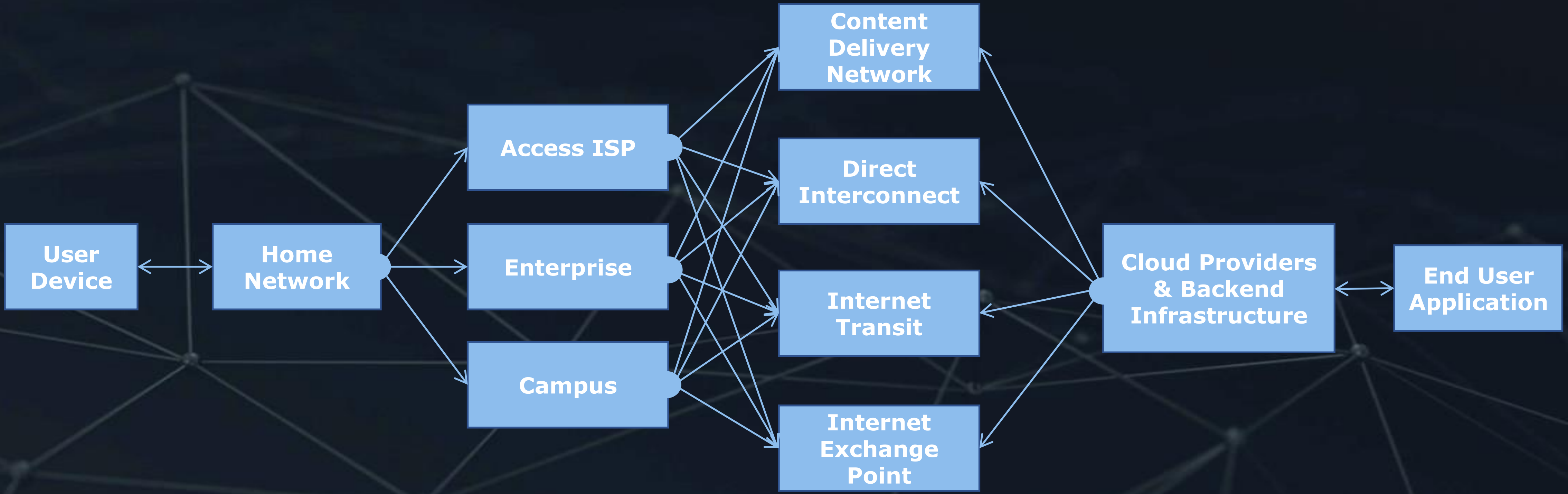
2013 – Chinese internet breakdown biggest DDoS

2016 – DYN IoT turned into botnets Mirai

2018 – GitHub 1.3 Tbps memcached over UDP

2018 – 1.7Tbps Memcached UDP New Record

COVID-19 impact on the Internet Ecosystem

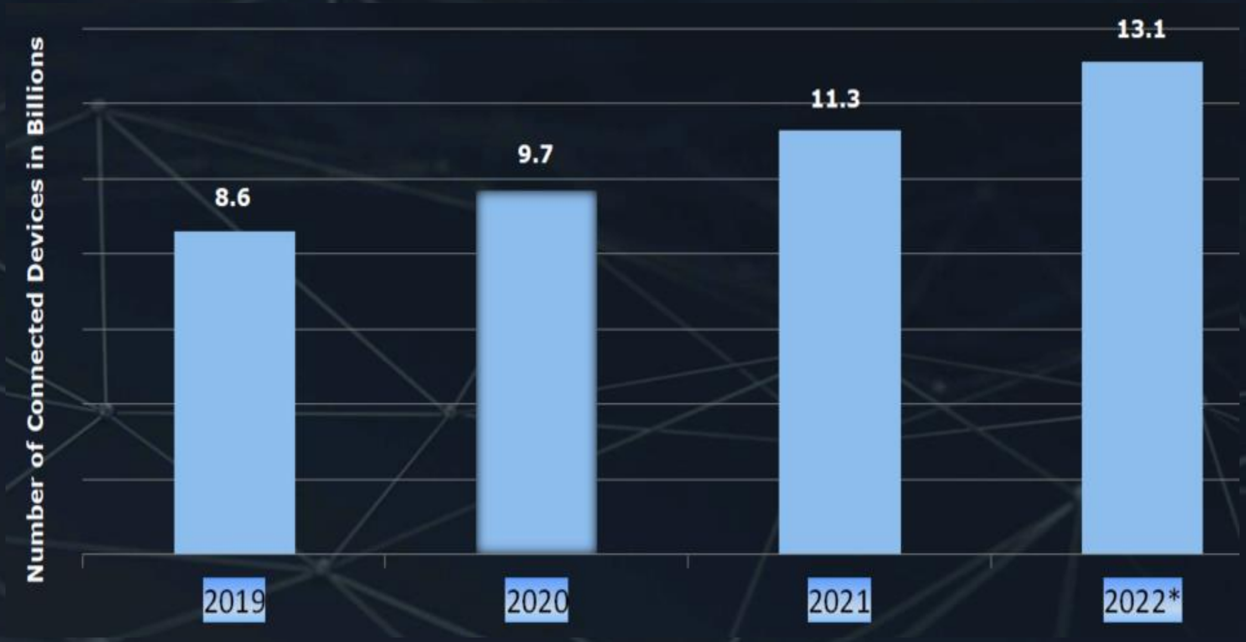


Simplified End-to-End Internet Ecosystem

PATH

COVID-19 immediate impact on the Internet Ecosystem

Number of Internet of Things (IoT) connected devices



ISP Networks

- Large cable operators – **DS 20% / US 35%**
- Small cable operators – **DS 27% / US 36%**
- Mobile operators – data usage increased **28.4%**

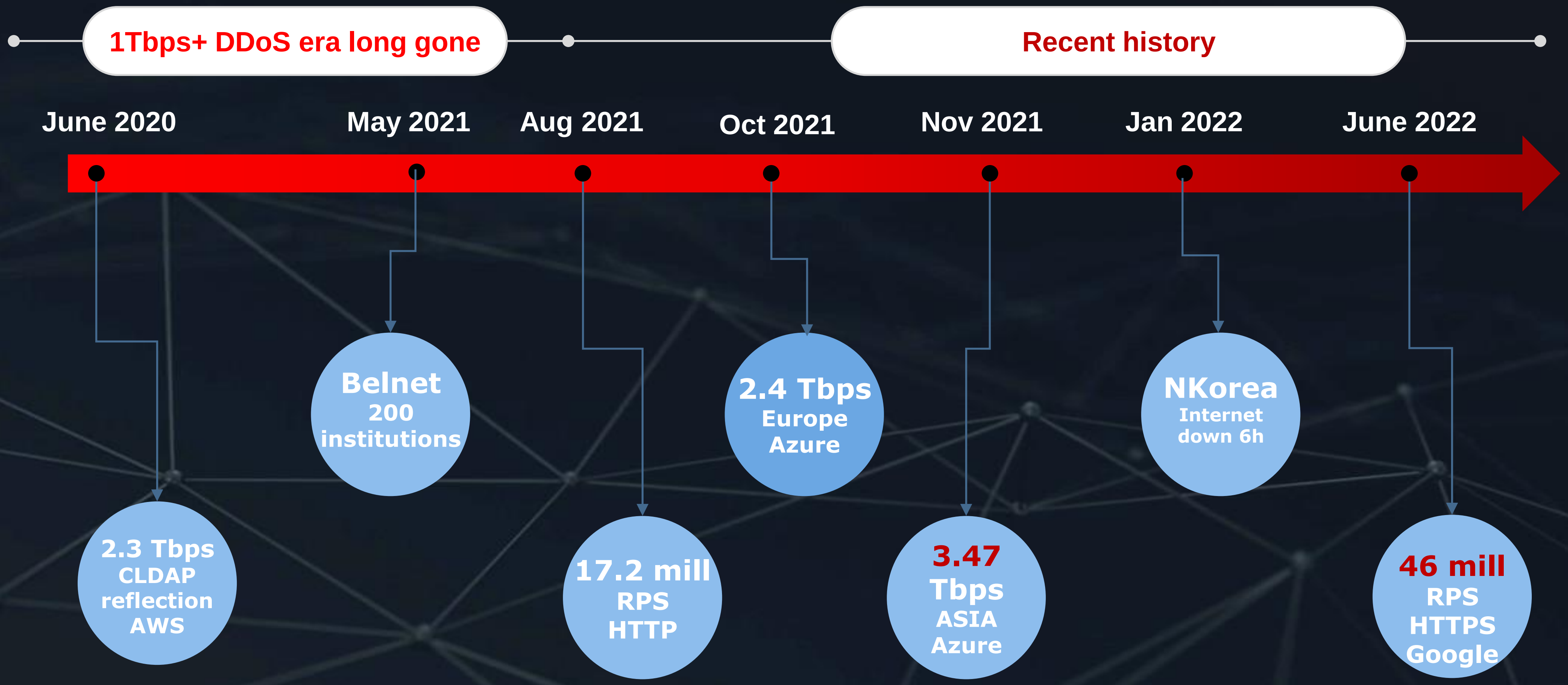
Transit Networks - 20% - 50%

Internet Exchange Points (IXPs)

- LINX - **40% / 6Tbps +**
- DE-CIX - **27% / 10Tbps +**
- AMS-IX - **35% / 9Tbps +**
- Interlan - **25% / 350 Gbps +**

PATH

DDoS attacks timeline during Covid19



1Tbps+ DDoS era long gone

Recent history

June 2020 — 2.3 Tbps CLDAP reflection AWS

May 2021 — Belnet 200 institutions

Aug 2021 — 17.2 mill RPS HTTP

Oct 2021 — 2.4 Tbps Europe Azure

Nov 2021 — 3.47 Tbps ASIA Azure

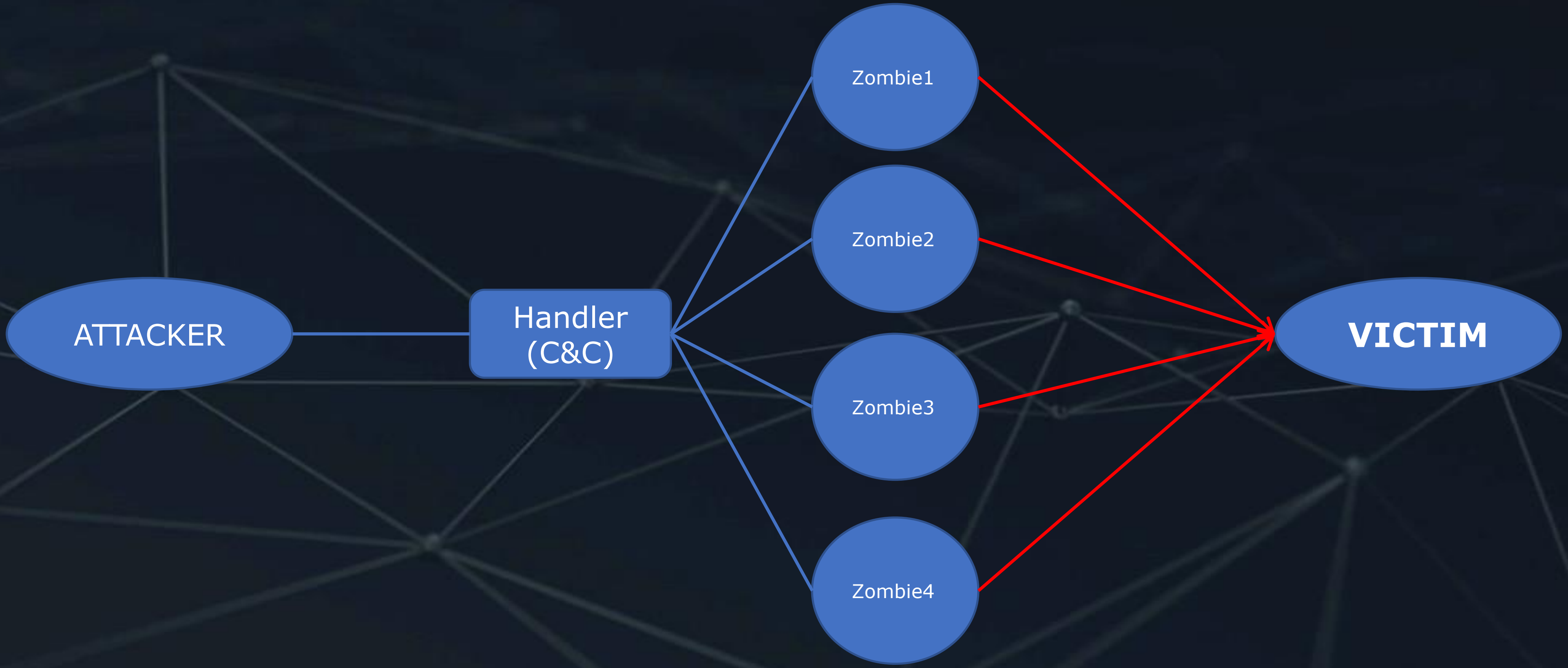
Jan 2022 — NKorea Internet down 6h

June 2022 — 46 mill RPS HTTPS Google

PATH

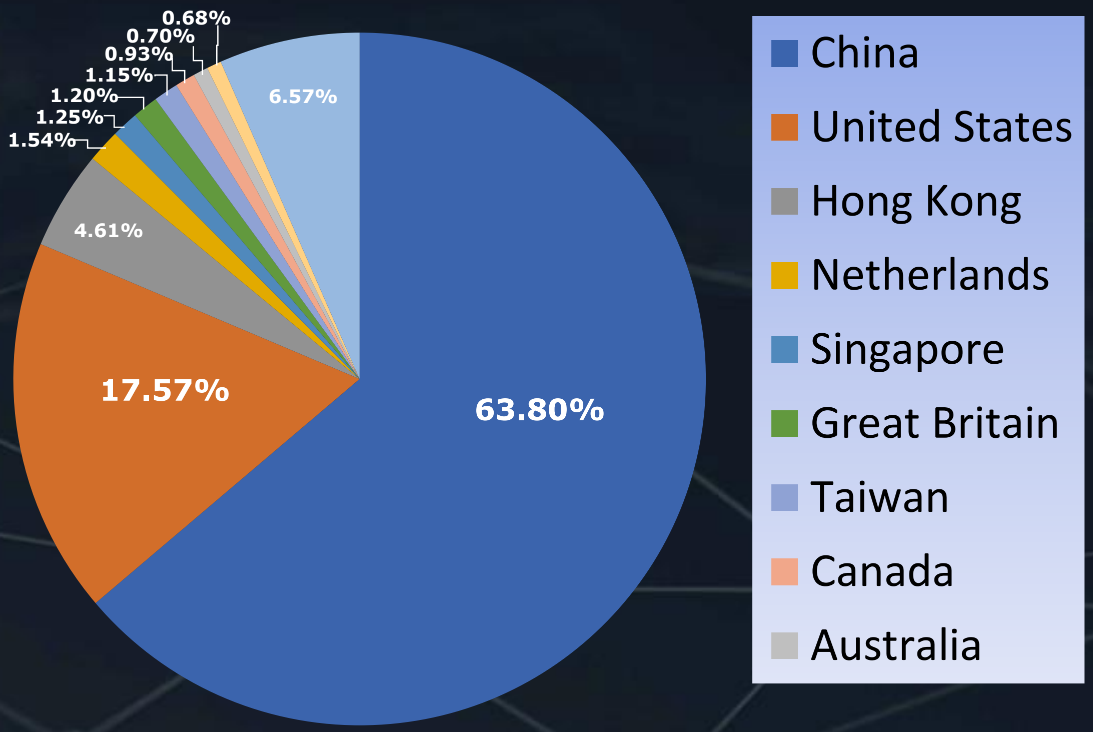
What is a DDoS attack?

DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server or a network with unsolicited internet traffic to prevent users from accessing connected online services and sites.

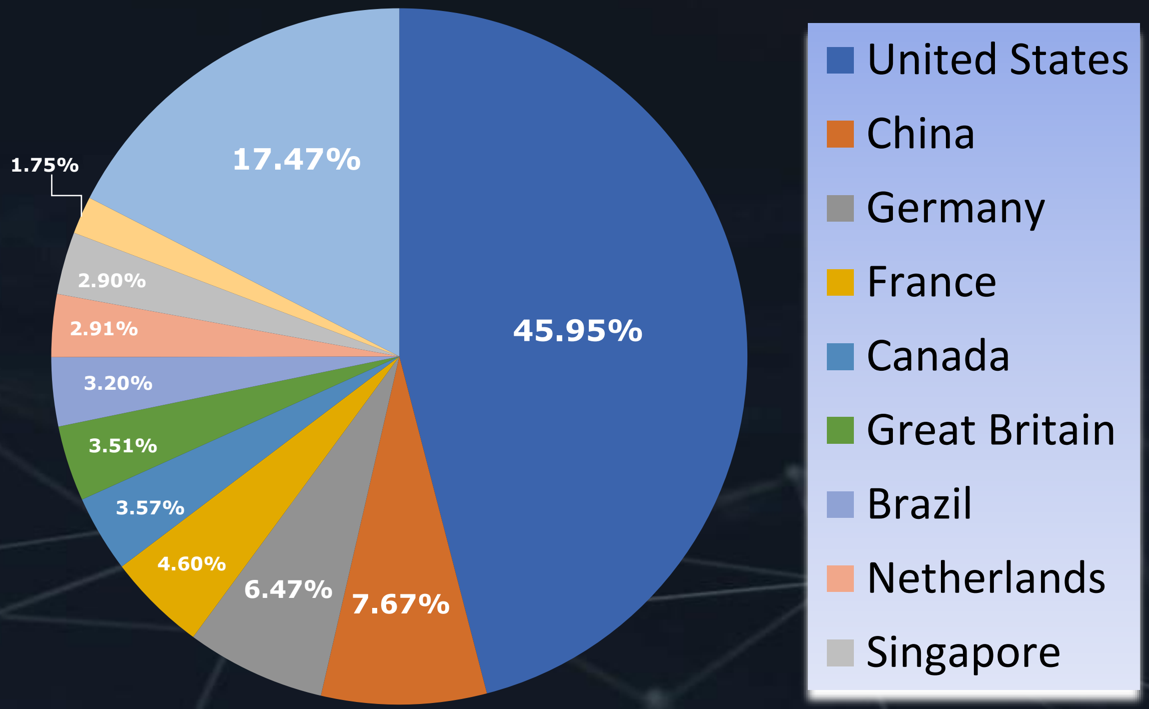


PATH

DDoS attacks destinations worldwide

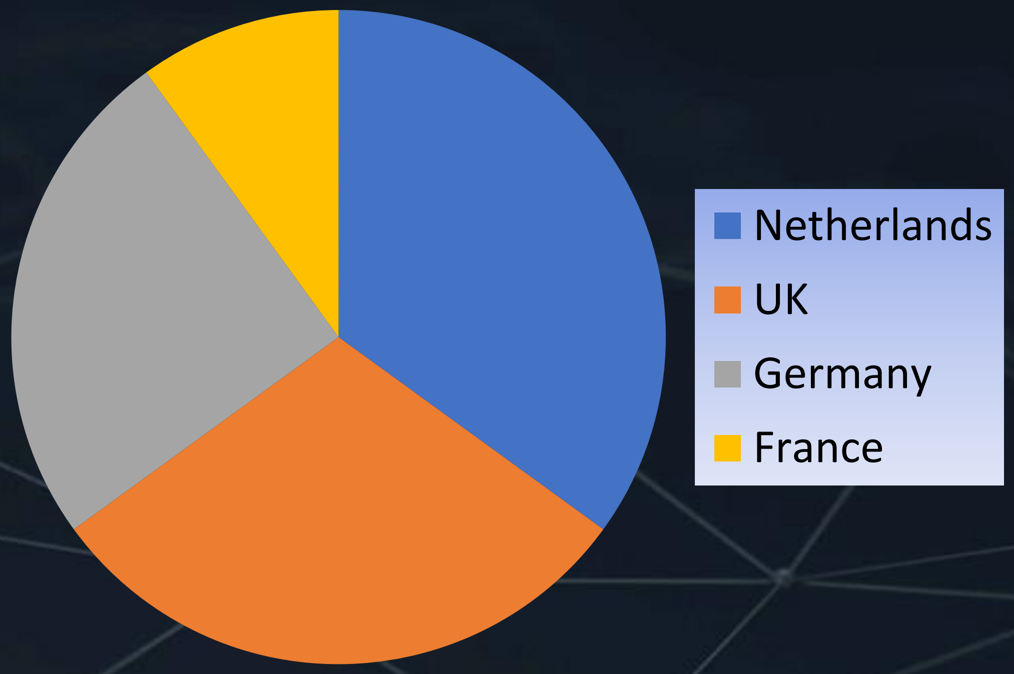


Q2 2019

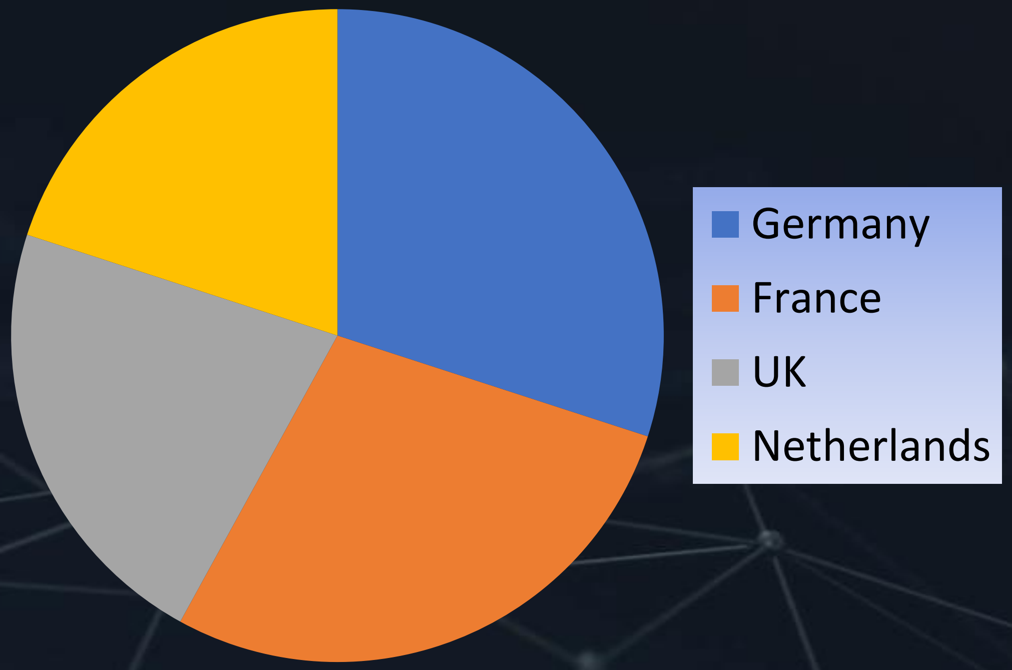


Q2 2022

DDoS attacks destinations Europe



Q2 2019



Q2 2022

PATH

Botnet distribution

China is a botnet hub with over 630,000 bots. United States is the second-worst, with almost 400,000 bots, followed by India, which has around the same.

The 10 Worst Botnet Countries	
China	631256
United States of America	394548
India	387281
Indonesia	197154
Thailand	194995
Algeria	128436
Brazil	89950
Vietnam	86540
Pakistan	84751
Japan	66804

The 10 Worst Botnet ASNs	
AS4134 - China_Telecom_(ChinaNet)	446514
AS16509 - AMAZON-02	348891
AS45609 - Bharti Airtel - GPRS	158482
AS4837 - China_Unicom	146813
AS36947 - Telecom_Algeria	108512
AS7713 - PT_Telekomunikasi_Indonesia	101564
AS14618 - Amazon AES	87952
AS24560 - Bharti Airtel Telemedia	67158
AS23969 - TOT Public	61697
AS17557 – Pakistan Telecommunication	46378

Botnet C&Cs geolocation distribution

Top 10 locations of botnet C&Cs	
United States	814
Russia	192
France	160
China	129
Germany	119
Luxembourg	95
Greece	79
Canada	73
Netherlands	66
United Kingdom	55

Q2 2019

Top 10 locations of botnet C&Cs	
Russia	1254
United States	384
Netherlands	216
Saudi Arabia	205
Germany	159
Mexico	137
Uruguay	100
Moldova	98
Dominican Rep	85
France	78

Q2 2022

52.41%↑

DDoS attacks by industry

2019

- Medium & large Telco
- Gaming
- Gambling
- IT services
- BFSI (Banking, Financial Institutions)
- Ecommerce

2022

- Medium & large Telco
- Gaming
- Gambling
- Public sector
- BFSI (Banking, Financial Institutions)
- Cryptocurrency / Blockchain companies

PATH

DDoS attacks by protocol type

2019

- 82.43% - SYN
- 10.94% - UDP
- 3.26% - TCP
- 2.77% - HTTP
- 0.59% - ICMP

2022

- 62.53% - UDP
- 20.25% - SYN
- 11.40% - TCP
- 3.29% - GRE
- 2.43% - HTTP

DDoS attacks by the numbers

Q2 2019

- 19 min – average duration of a DDoS session
- 21 days – longest DDoS session
- 10X– increase of DDoS >100Gbps between 2019 – 2020
- 20% – multi vector DDoS attacks from the total
- 1.7 Tbps – biggest DDoS attack to date

Q2 2022

- 3000 min (2 days) – average duration of a DDoS session
- 29 days – longest DDoS session
- 6.5X – increase of DDoS >100Gbps between 2020 - 2022
- 78% – multi vector DDoS attacks from the total
- 3.47 Tbps – biggest DDoS attack to date

DDoS security trends & predictions

- DDoS attacks - more complex
- Smaller DDoS attacks are on the rise
- L7 smart attacks are on the rise
- IoT devices to reach 29.4 billions by 2030
- Mitel MiCollab – amplification method - 4 billion-fold amplification potential
- New records in DDoS attack size and duration

PATH

The cost of a DDoS attack

DDoS For Hire

- $20 /month – 10Gbps L4&L7
- $85 /month – 50Gbps L4&L7
- $1000 /month – 200Gbps L4&L7
- $13000 /month ~1Tbps DDoS L4&L7 / 6-12 hours sustained attack
- SLA 80%

Ransomware

- $5000 – small business
- $25000 – medium business
- $170000 – enterprise
- 20X when combined with encryption-based ransomware
- 32% pay the ransom

Impact

- $8,000 - $74000 /hour – online retailers
- $120,000 – SMB cost of restoring service
- $5,500 /min – SMB downtime cost
- Up to $300,000 /hour cost of global network company
- Customer trust

PATH

Available solutions

Blackholling

- Configures rules at core layer
- Both legitimate and malicious traffic is dropped from the network
- Still widely available for small and medium networks
- Major traffic disruption
- Not DDoS mitigation

Software (Flowspec)

- Installed on premise and in neighboring networks
- Full control over traffic
- Requires very advanced networking skills
- Extra bandwidth costs with upstream providers
- Works well with already known types of DDoS

Hardware

- Placed inline in client's network (on-premise)
- Vendor specific
- Requires trained personnel
- Works well for smaller attacks and L7
- Works well with already known types of DDoS
- CAPEX intensive

Cloud-based scrubbing

- BGP based
- Redirects traffic to the closest scrubbing center
- On-demand & always on
- Works well for volumetric attacks
- Delivered as a service (direct link or GRE)
- Saves cost

THANK YOU

PATH NETWORK