NETSCOUT | Arbor

DDoS Wargames

23th October 2018

Michele Di Dedda – Consulting Engineer Italy & Greece

Alessandro Bulletti – Consulting Engineer Italy & Greece

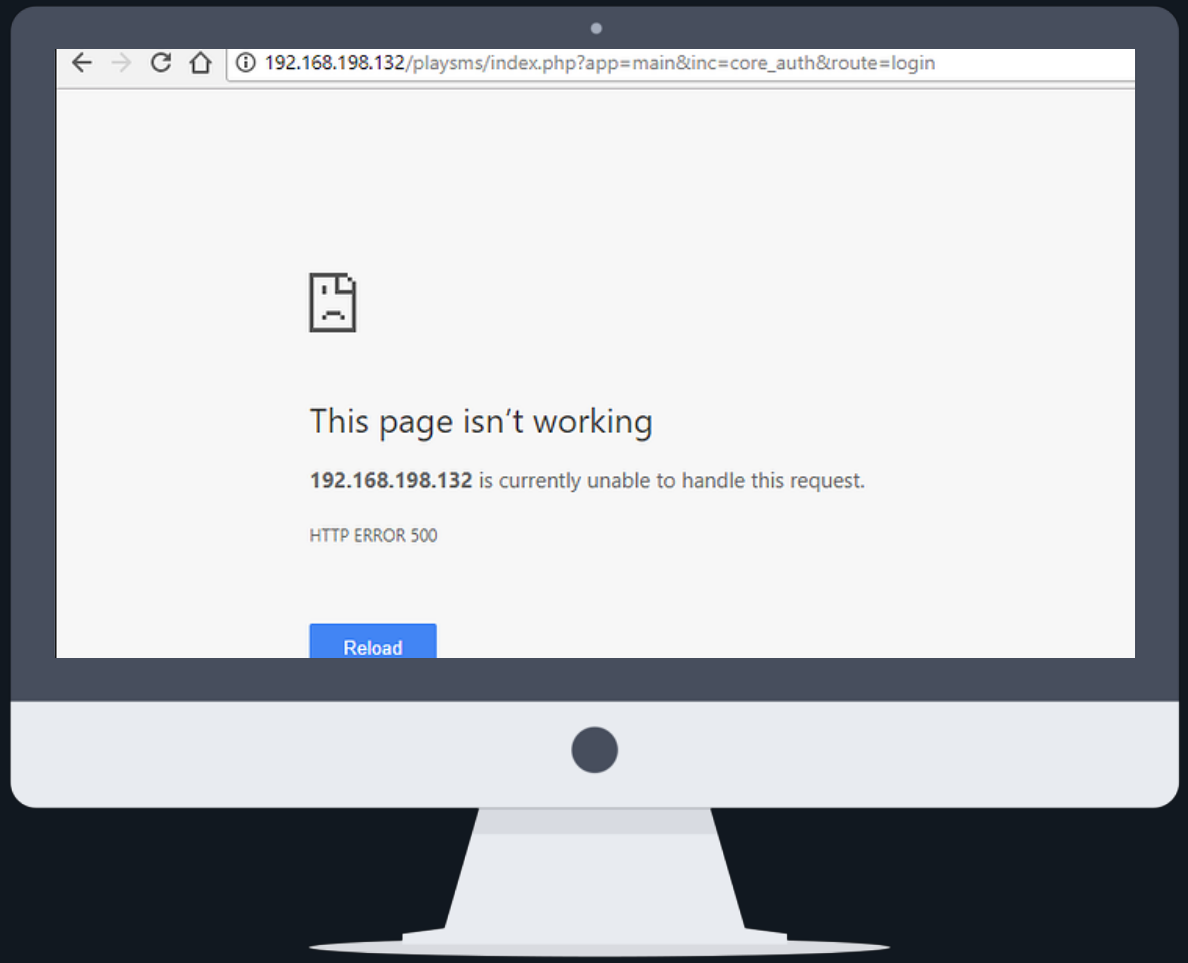
Agenda

- Why are we here today?
- Who are we?
- DDoS in the real world
- But how do I build my defense?
- Arbor SP and Arbor APS Demo

Why are we here today?

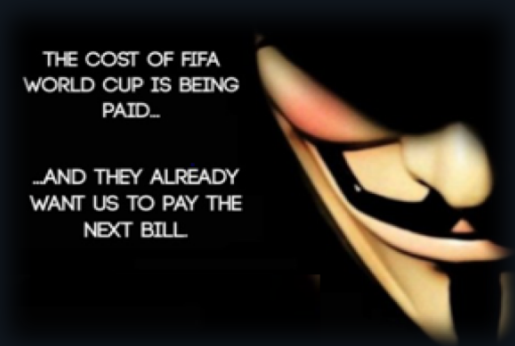
- Distributed Denial of Service

- To exhaust resources
- To prevent legitimate users to connect



The Cyber Reflection

Every event has a cyber reflection



Attack targets were not necessarily the events themselves,
but organizations tangentially associated with the events.

What is it used for?

Attackers - Victims

- Mafias
- Hactivists
- Competition
- Gamers
- Students
- Former employee
- Ransom
- Political Statement
- Business impact
- Get rid off the opponent
- To skip tests
- Angry, Vengeance

"A 17-year-old high school boy may face state and federal charges for allegedly having paid a third party to launch a distributed denial of service (DDoS) attack that crippled the West Ada school district in Idaho, US, for a week and a half earlier this month."

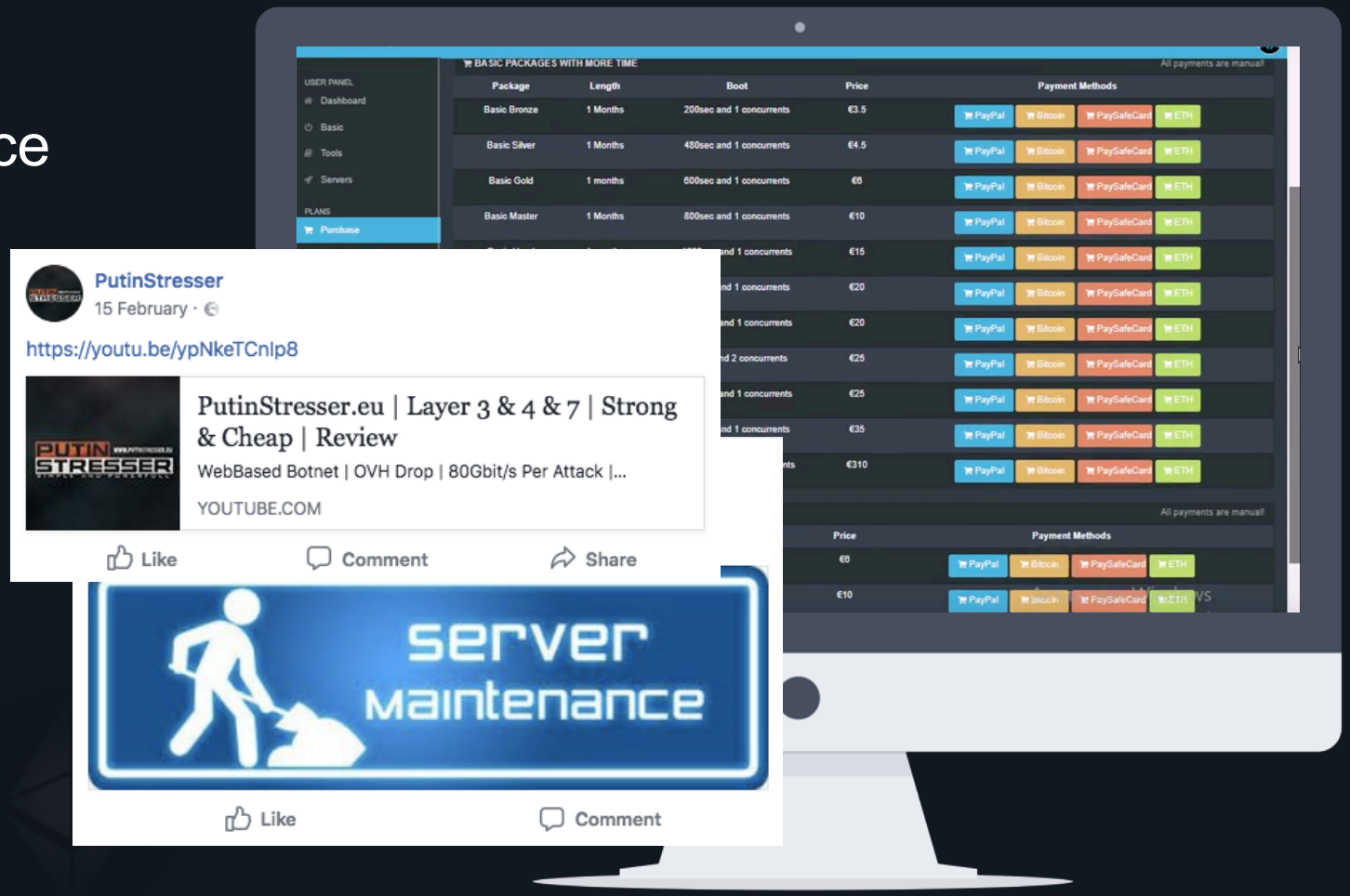
Some students had to take the tests multiple times.

Source: Naked Security

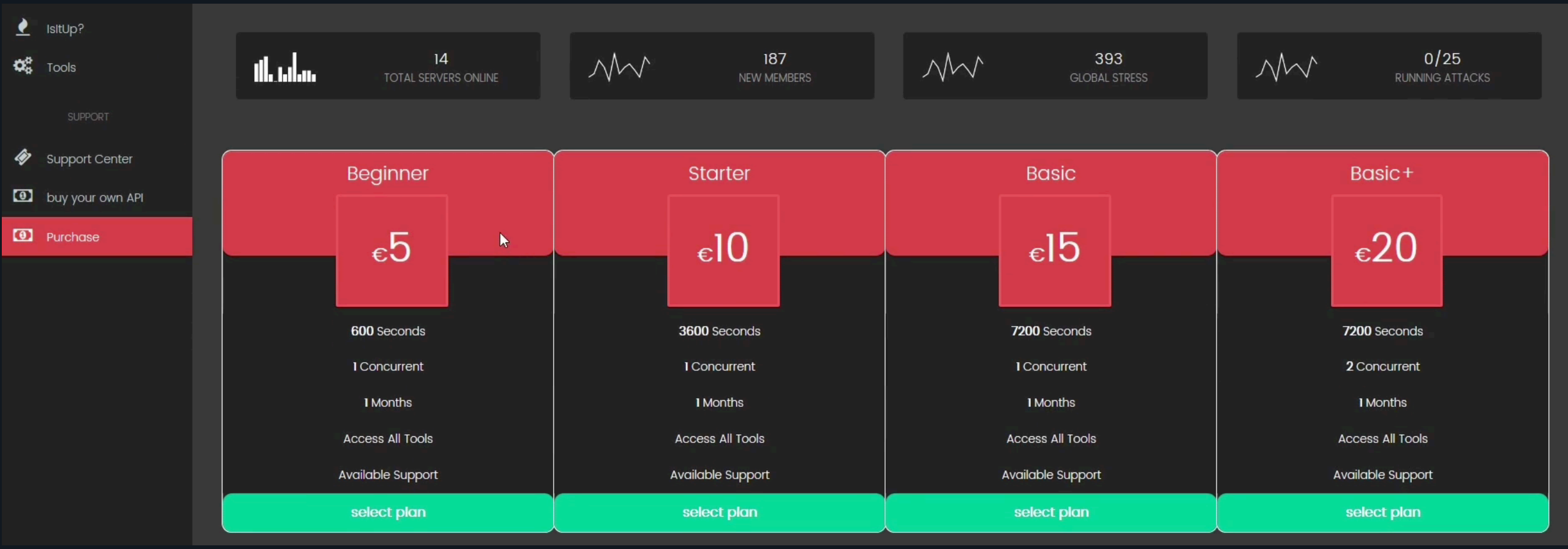
How easy it really is to launch a DDoS?

Really really easy!!!

- Easy to find
- Clear and modern User Interface
- Several locations
- Many attack vectors
- Multiple paiement options
- Support center
- Community Manager



Plans, service, support, APIs,



source: https://youtu.be/aLMEhEUPlds

Dutch banks crippled by DDoS Attack

January 2018

Myth:

ABN Amro CEO Kees van Dijkhuizen said that “attacks like these probably cost the perpetrators **tens of millions of euros**”, fuelling speculation that the attack had come from a **nation state**.

Fact:

But the truth has proved rather less spectacular when police arrested an **18-year-old** known as Jelle S in his home town of Oosterhout. Jelle claimed to have bought a ready-made “stresser” DDoS package on the dark web for which he had paid **€50 a week** to send **50-100Gb/s** of data to victims.

Source: computerweekly.com

NETSCOUT | Arbor

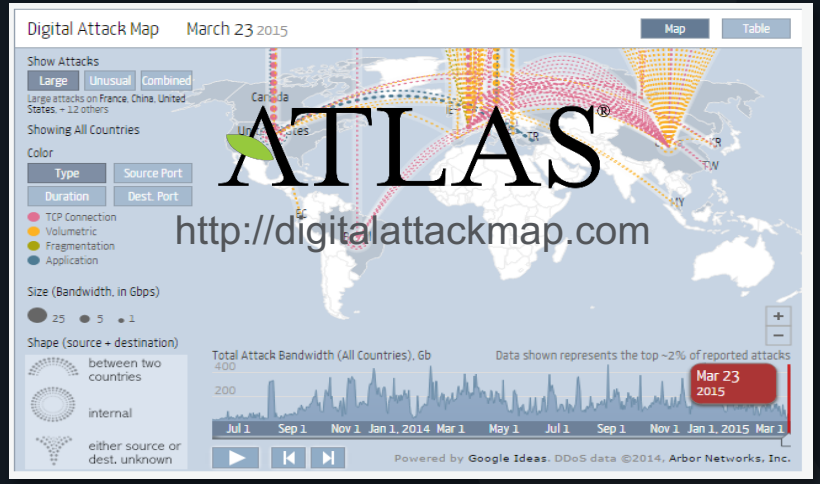
18 Number of years Arbor has been delivering innovative security and network visibility technologies & products

#1 Industry leader in DDoS attack protection products.

98% Percentage of world's Tier 1 service providers who are Arbor customers

1/3 = Amount of Internet traffic monitored by the ATLAS

NTT · at&t · TATA · verizon · 中国电信 CHINA TELECOM · T-Com · Telefónica · vodafone · BT · orange

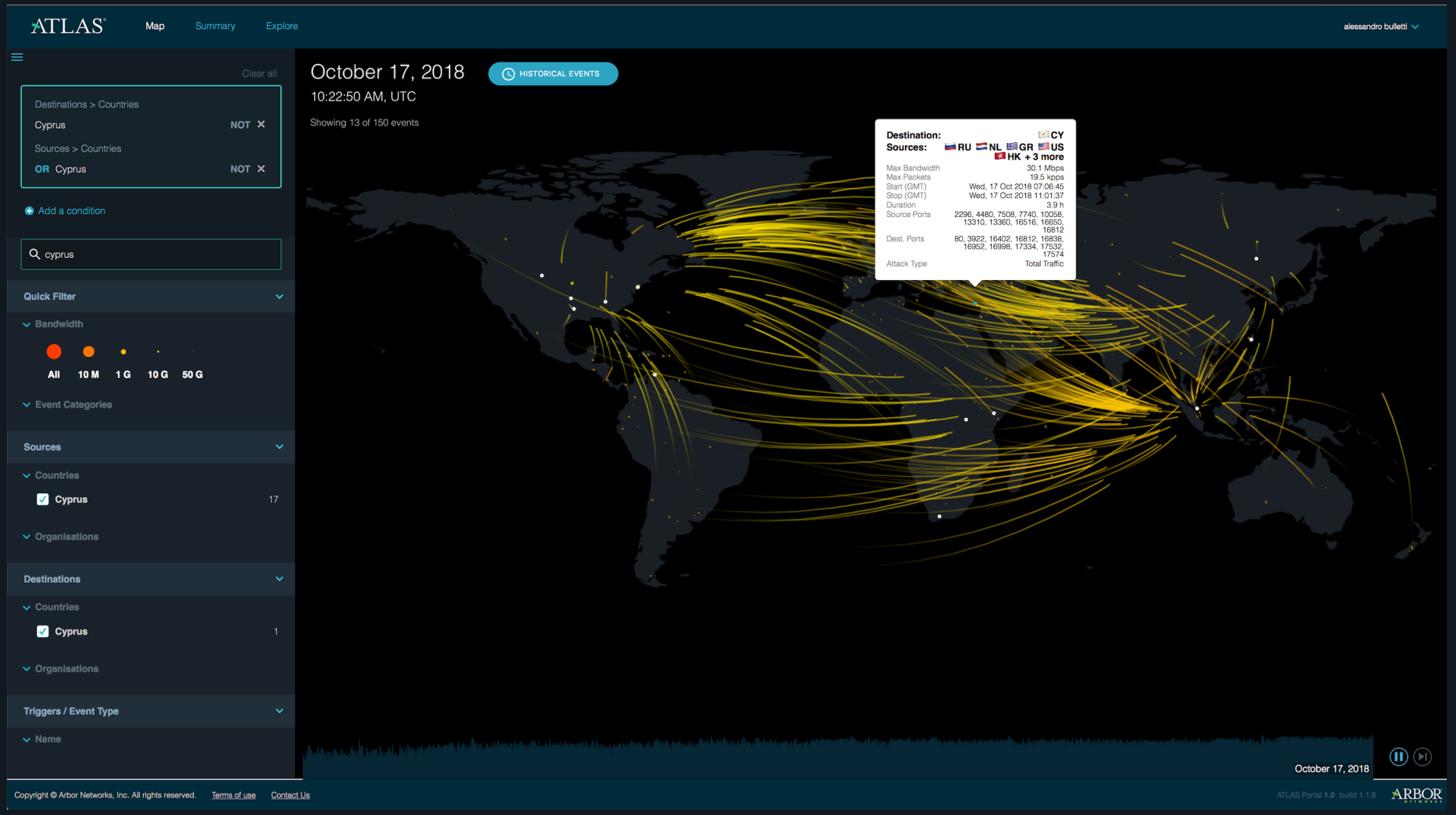


Arbor Networks knows more about the internet's workings than possibly anyone outside the National Security Agency.

Ryan Singel – Wired.com

ATLAS Data collects stats at any time

- Cyprus as S/D Country view on October 17th

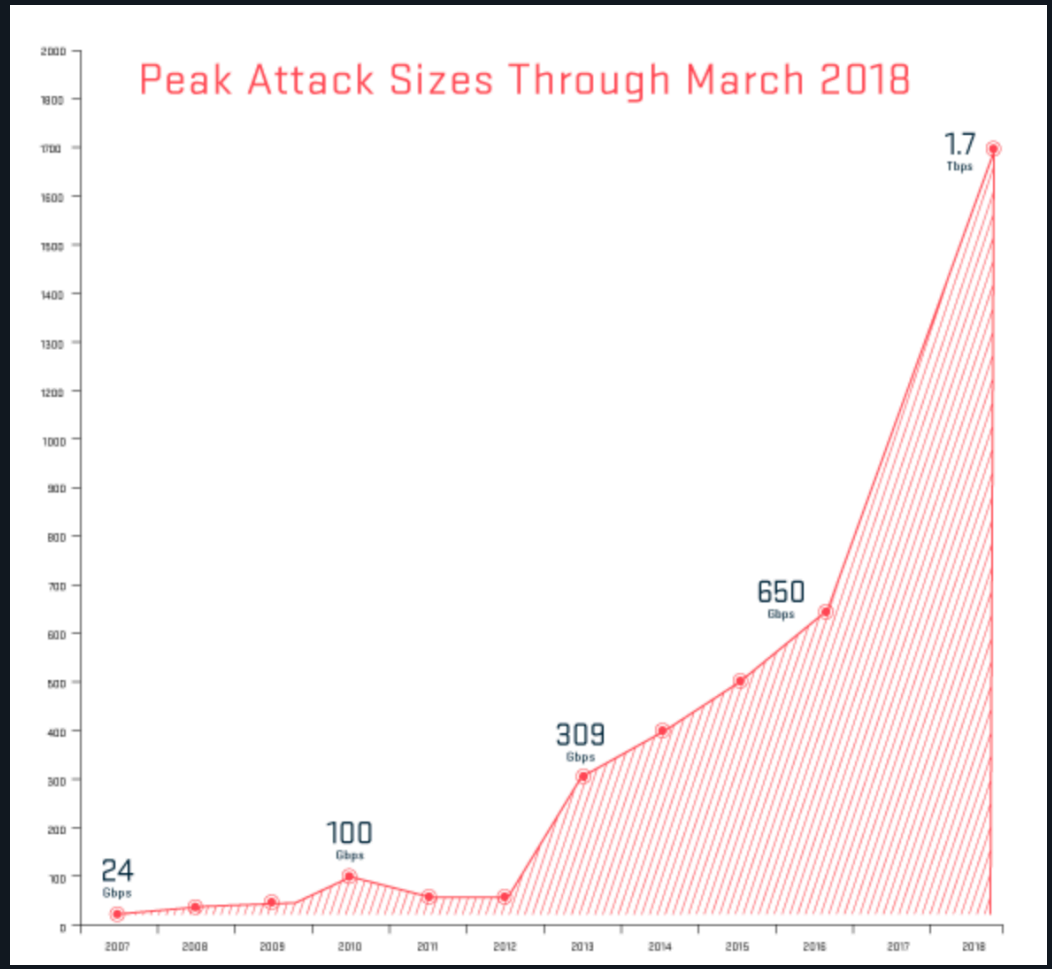


Peak attacks

2018 is a record year…

- New weaponized attack vectors like memcached
- Targets a vulnerability in a Datacenter service used to improve request performance
- Amplification factor can go up to 1:500,000 (maximum achieved in a lab environment)
- 1Mbps can generate 50Gbps

- **Not the most dangerous attack**



Attack Frequency

- ATLAS observed 7.5 million DDoS attacks in 2017 vs. 6.8 million in 2016
- 10% surge in a year
- DDoS is the easiest attack you can launch
- DDoS is the cheapest attack you can launch
- Few prosecution
- *ATLAS attacks observed for Cyprus, from Oct 2017 to present*

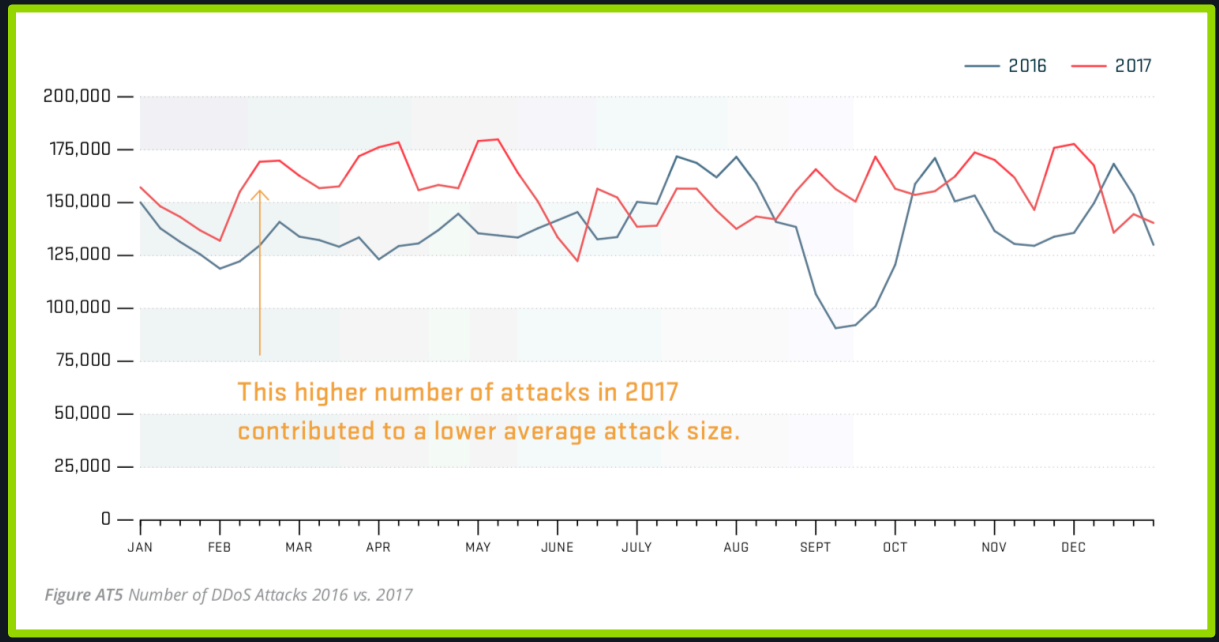
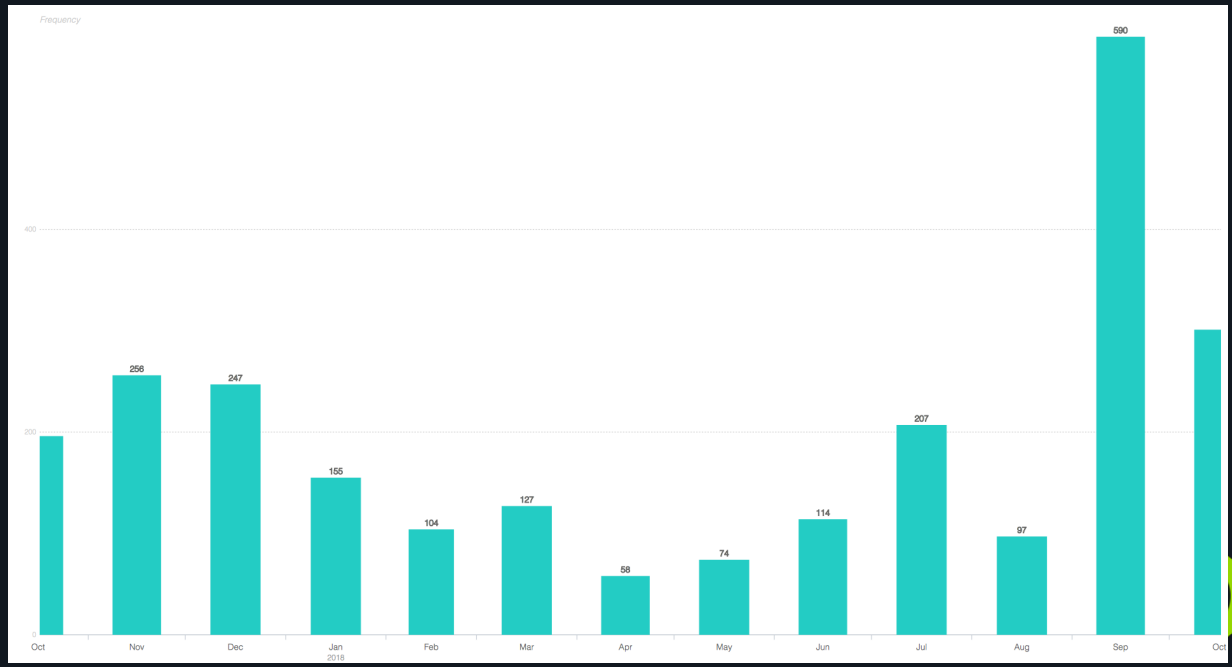


Figure AT5 Number of DDoS Attacks 2016 vs. 2017



How many times have you been attacked?

Out of a panel of 400 entreprises

Figure 65 DDoS Attack Frequency

Most used mitigation tools are the least effective

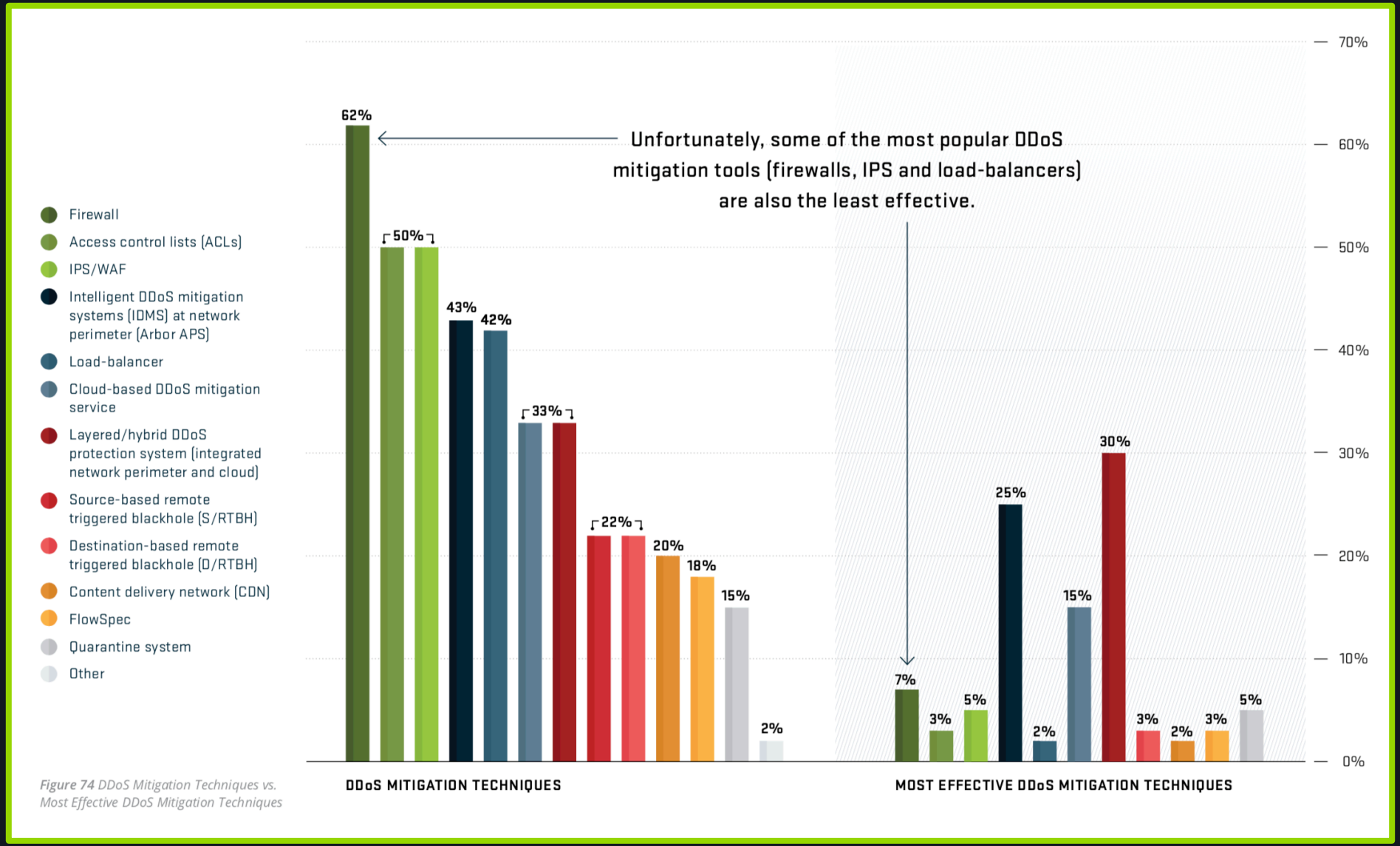
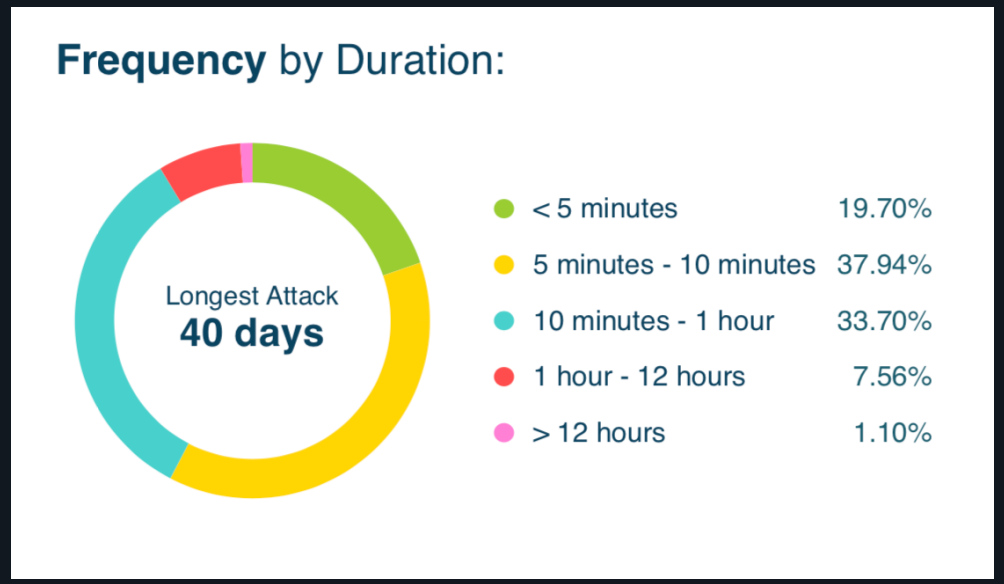


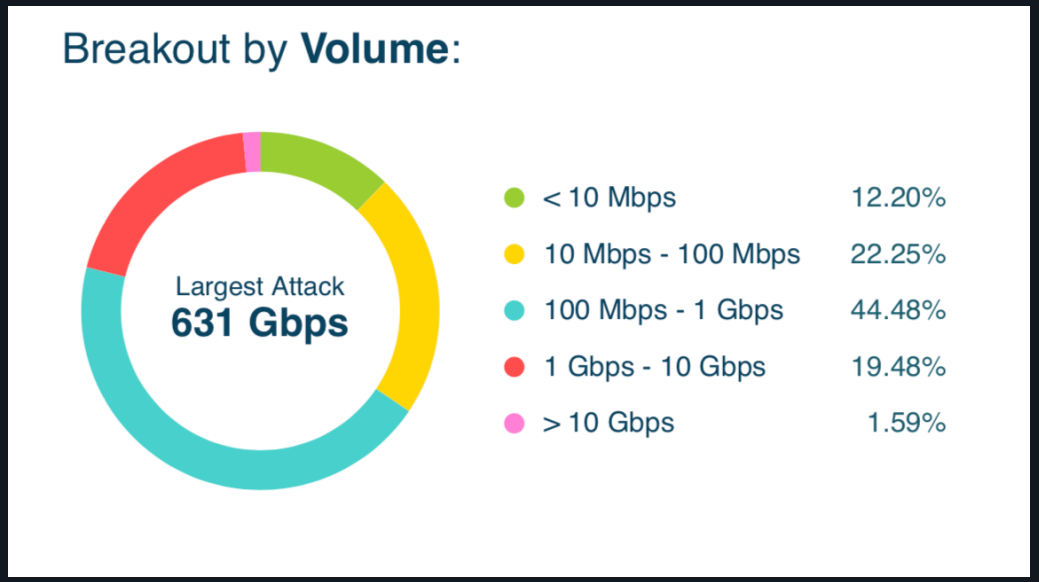
Figure 74 DDoS Mitigation Techniques vs. Most Effective DDoS Mitigation Techniques

Trend for DDoS Attacks

- WW data per September 2018 as collected by ATLAS
- Frequency and Breakout by Volume indicate short attacks
- Average bandwidth still < 1G

Remember, attacks are getting more complex

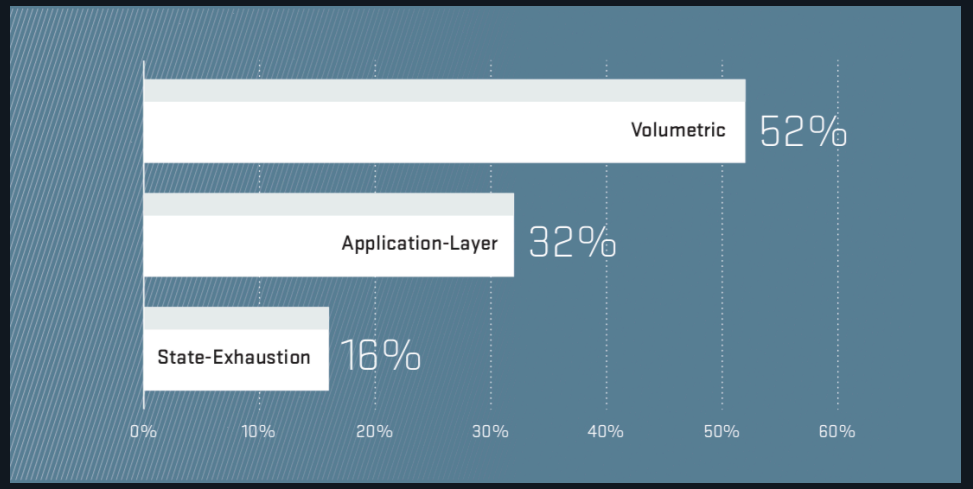




Complexity and subtlety

DDoS attacks are organic

- DDoS attack change during the attack
- The attacker keeps an eye on the victims resources availability
- The vector will change to defeat the countermeasures
- 48% of attacks can be stopped on site
- 52% may require help from the ISP



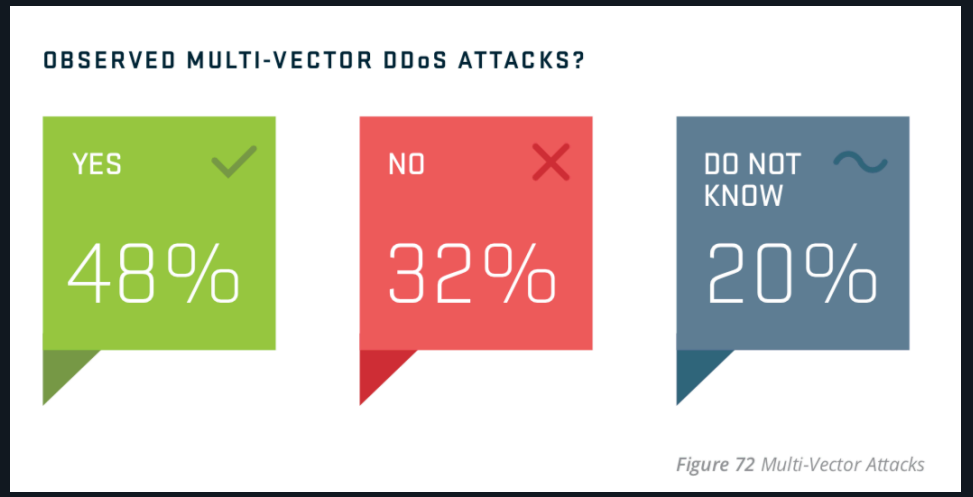


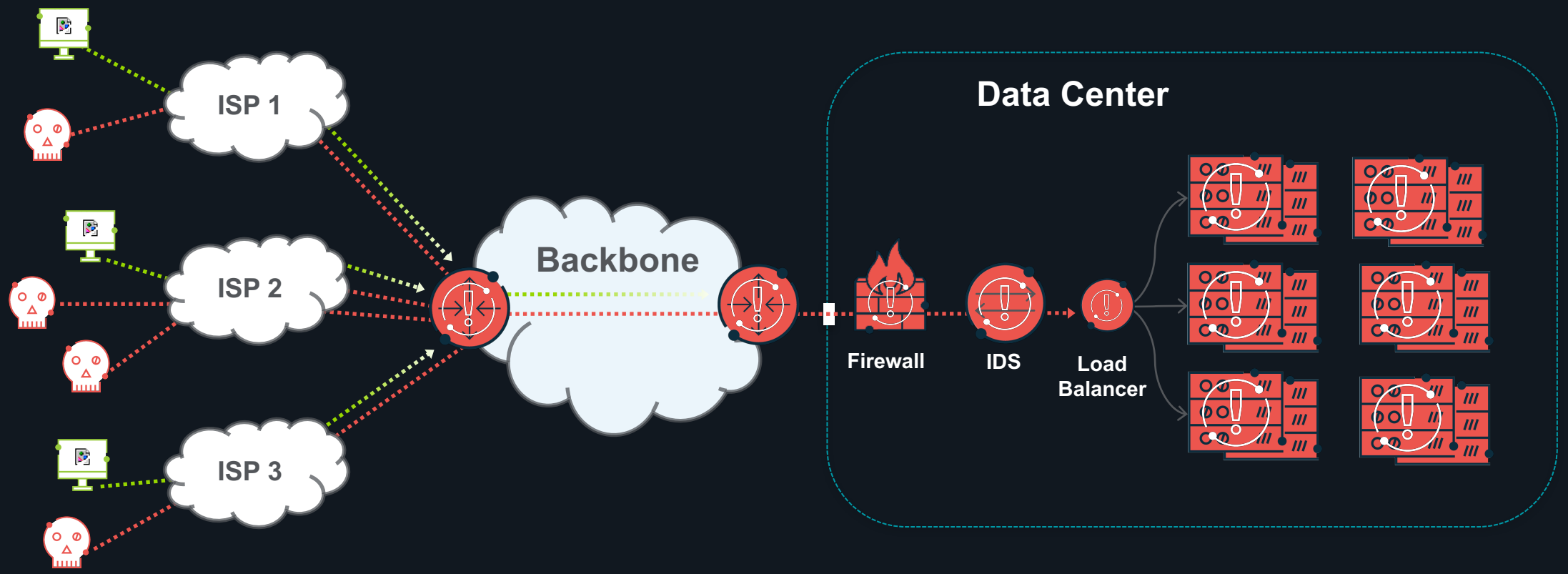
Figure 72 Multi-Vector Attacks

Time to mitigation

More important than you might think

- Reducing the time to mitigation will benefit your company in several ways
- The infrastructure will not be impacted by any collateral damage (firewall, ips, waf crashing)
- The service will stay available longer
- Your customers won’t leave

How to counter every type of attack

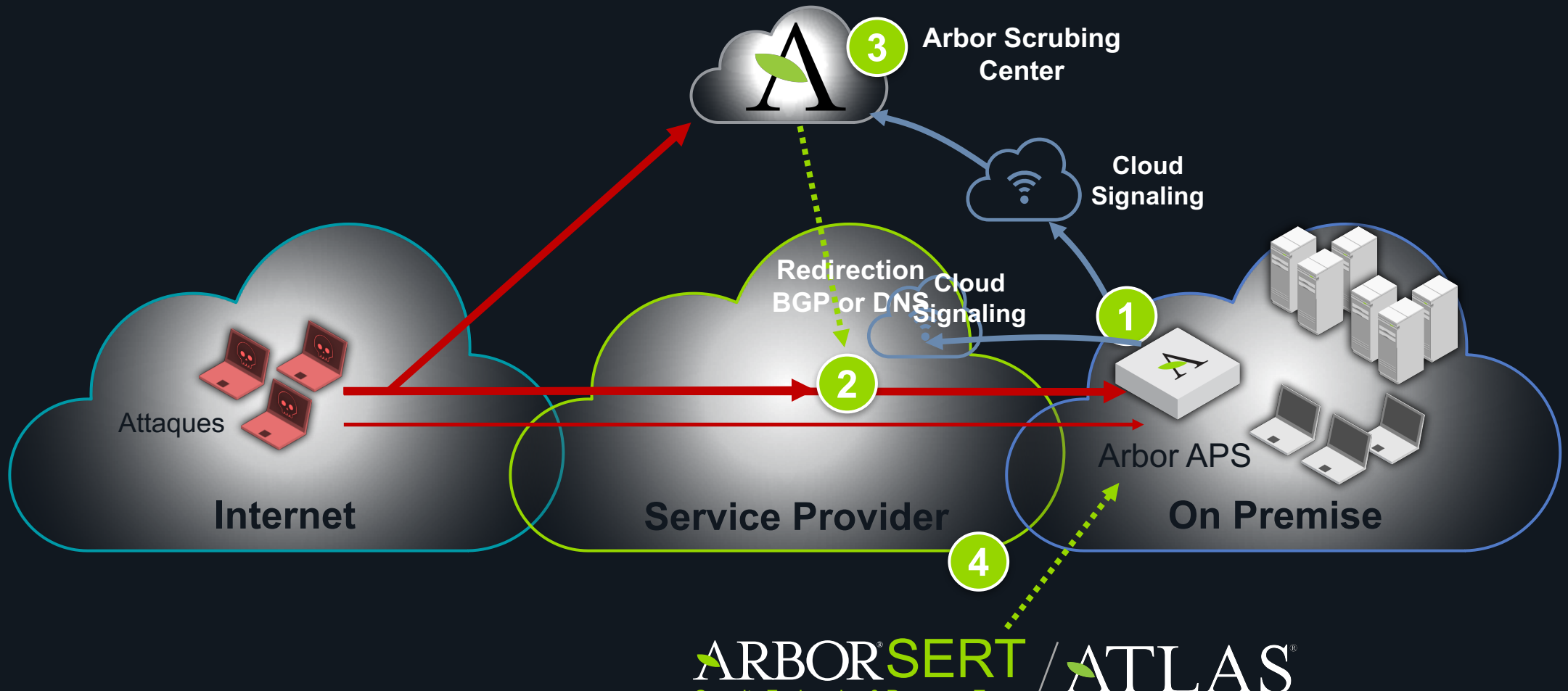


Saturation
Volumetric or Flooding Attack

Exhaustion of State
L4 – L7
Crashes stateful devices (Load Balancers, Firewalls, IPS/IDS)

Exhaustion of Service
L4 – L7
Application Layer or Slow & Low Attack, Crashes application servers

Arbor's Unique Multi-Layer DDoS Approach



Backed by the industry

SANS EMEA

*"DDoS mitigation solutions integrating on-premise equipment and ISP and/or mitigation architectures are nearly **four times more prevalent** than on-premise or services-only solutions."*

*"...**Hybrid DDoS solutions offer best-of-breed attack mitigation** by combining on premise and cloud mitigation into a single, integrated solution..."*

THALES

FORRESTER®

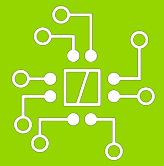
***"Hybrid solutions offer the best of both**. (…) A hybrid approach provides fast detection and defense with low latency with the ability to utilize cloud-based mitigation should the need arise."*

*"As DDoS attacks become more complex, **it becomes critical to ensure that the defenses become more integrated**. This trend for on-premises combined with off-premises, or **hybrid DDoS defense**, has become the strategy for many of the vendors."*

Gartner®

Best Practices

1

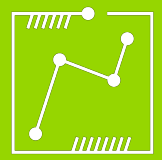


- Factor network availability into the design of online services or applications; continuously stress-test.

2

- Develop a DDoS Attack Mitigation Process
- Continuously stress-test & refine.

3



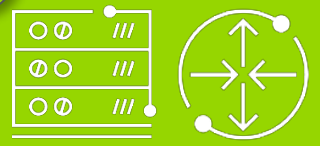
- Utilize flow telemetry (e.g. NetFlow) collection & analysis for attack detection, classification & trace back.

4

Deploy multi-layered DDoS protection which includes:

- On-premises Intelligent DDoS Mitigation Systems (e.g. Arbor APS / TMS products)
- Overlay cloud-based DDoS protection services (i.e. Arbor Cloud or ISP/MSSP)
- Network infrastructure-based techniques such as S/RTBH & Flowspec at all network edges

5



- Scan for misconfigured, abusable services running on servers, routers, switches, home CPE devices, etc. (i.e. TCP 23/2323). Alert users running abusable services – possibly blocking until they are remediated.

Best Practices

6 NTP Services

- Check Open NTP Project for abusable NTP services on your networks.
- Disallow Level 6/7 NTP queries from the Internet.

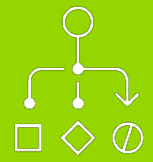
7 DNS Recursors

- Check Open Resolve Project for abusable open DNS recursors on your networks. Ensure only authorized users can query recursive DNS servers.

8

- Ensure SNMP is blocked on public-facing infrastructure/ servers.

9



- Employ Anti-spoofing mechanisms such as Unicast Reverse-Path Forwarding, ACLs, DHCP Snooping & IP Source Guard, Cable IP Source Verify, etc. on all edges of ISP and enterprise networks.

10

- Participate in the global operational security community and share threat intelligence and defense best practices.

Thank You.

www.netscout.com

Guardians of the Connected World