ARBOR NETWORKS

The Security Division of NETSCOUT

An Introduction to DDoS attacks trends and protection

Alessandro Bulletti
Consulting Engineer , Arbor Networks
abulletti@arbor.net

Topics Covered

- The DDOS cyber threat and impacts
- Cyprus attacks trend in 2016
- How to address DDoS Challenges

Things you should know about DDoS attacks

- **It’s never been easier to launch a DDoS attack.**
- **DDoS attacks increasing in size, frequency and complexity.**
- **DDoS attacks are used as smoke screens diversion during advanced threat campaigns.**
- **Of the Top 3 causes of unplanned outages, DDoS attacks are the most costly to an organization.**

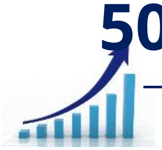
Did You Know?

$5:$100sK

DDoS for Hire

For $5/hr anyone can launch a DDoS attack an cause $100sK in damage

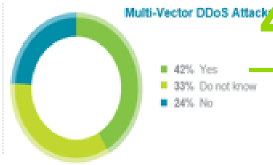
500Gbps



...DDoS attack size increasing [1]

74%

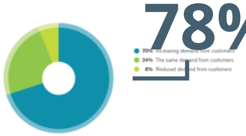
...involved DDOS as a diversion[2]



42%

...experienced multi-vectored attacks[1]

78%



...Increase in demand for DDoS Protection services[1]

DDoS background

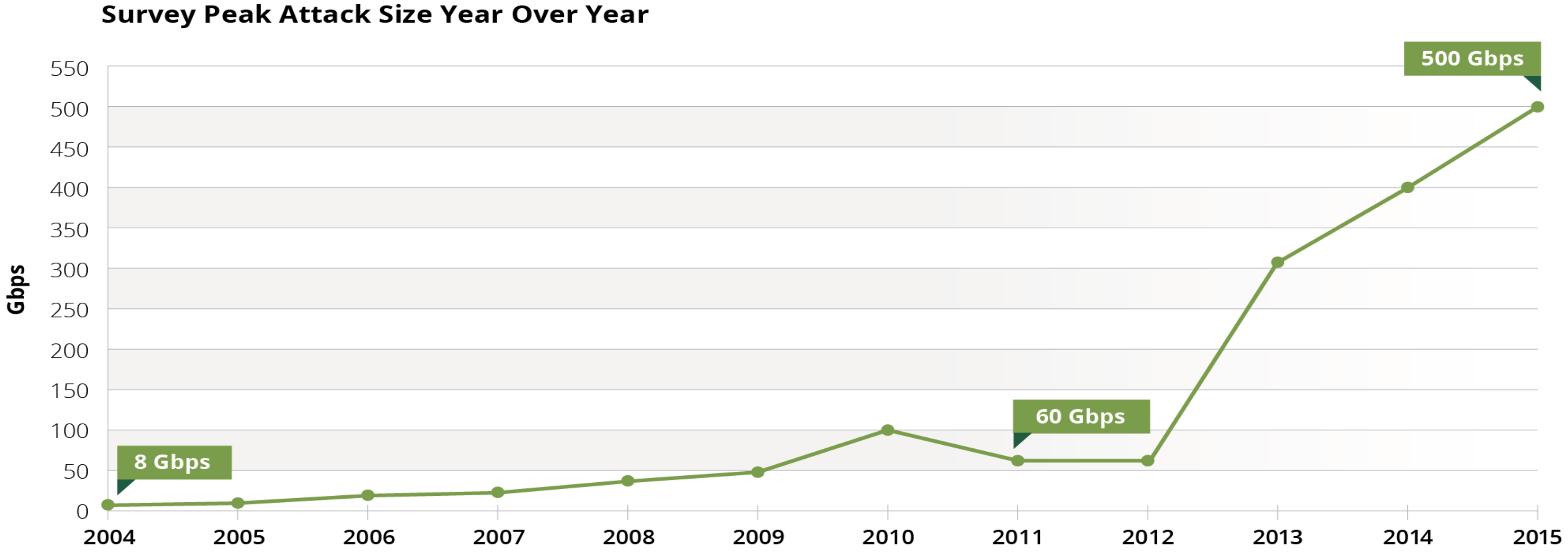
- **What is a DDoS “ Distributed Denial Of Service” attack?**

- **An attempt to consume finite resources, exploit weaknesses in software design or implementations, or exploit lack of infrastructure.**
- **An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.**

- **DDoS attacks effect availability! No Availability, no applications/services/data/internet! NO revenue!**

- **Attacks are almost always distributed for more significant effect**.

DDoS Growth continues

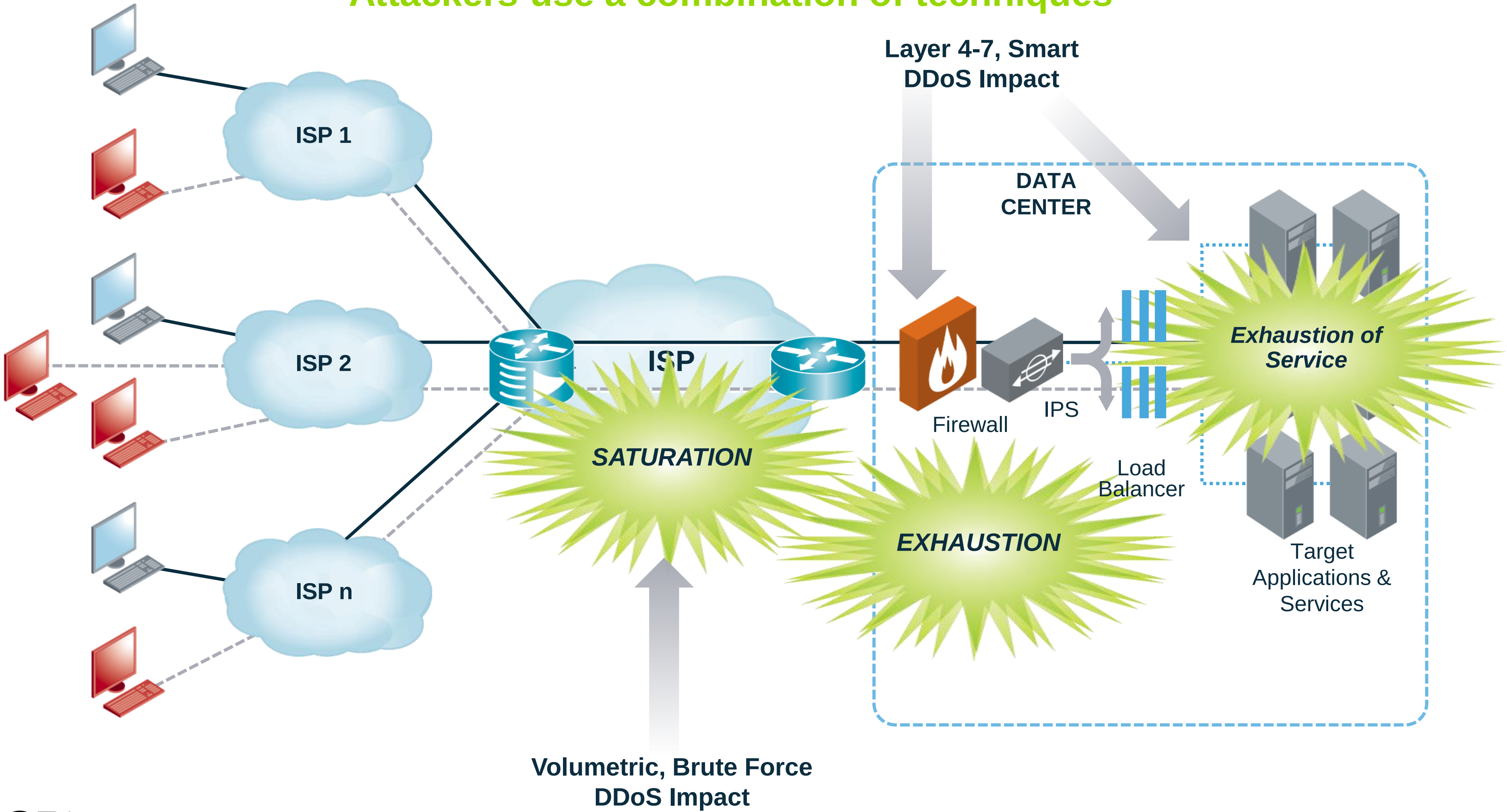


Source: Arbor Networks, Inc.

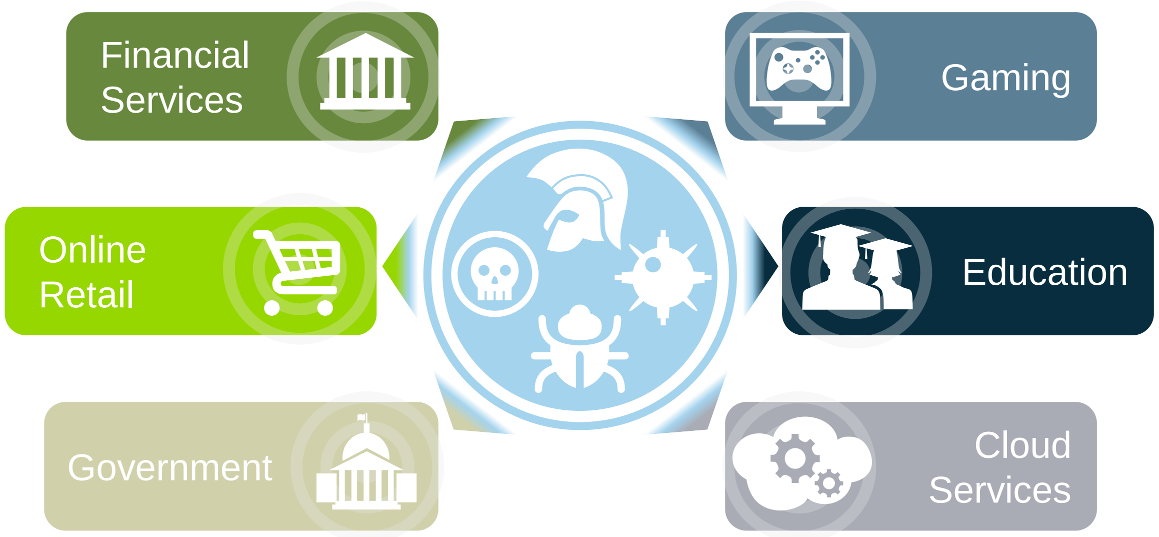
- Largest attack reported in 2015 was 500 Gbps with other respondents reporting attacks of 450 Gbps, 425 Gbps, and 337 Gbps.
- Another five respondents reported 200+ Gbps attacks.
- Nearly one quarter of respondents report peak attacks over 100Gbps.
- Over half of data center respondents saw attacks that completely saturated their Internet connectivity.

DDoS as an Evolving Threat

Attackers use a combination of techniques

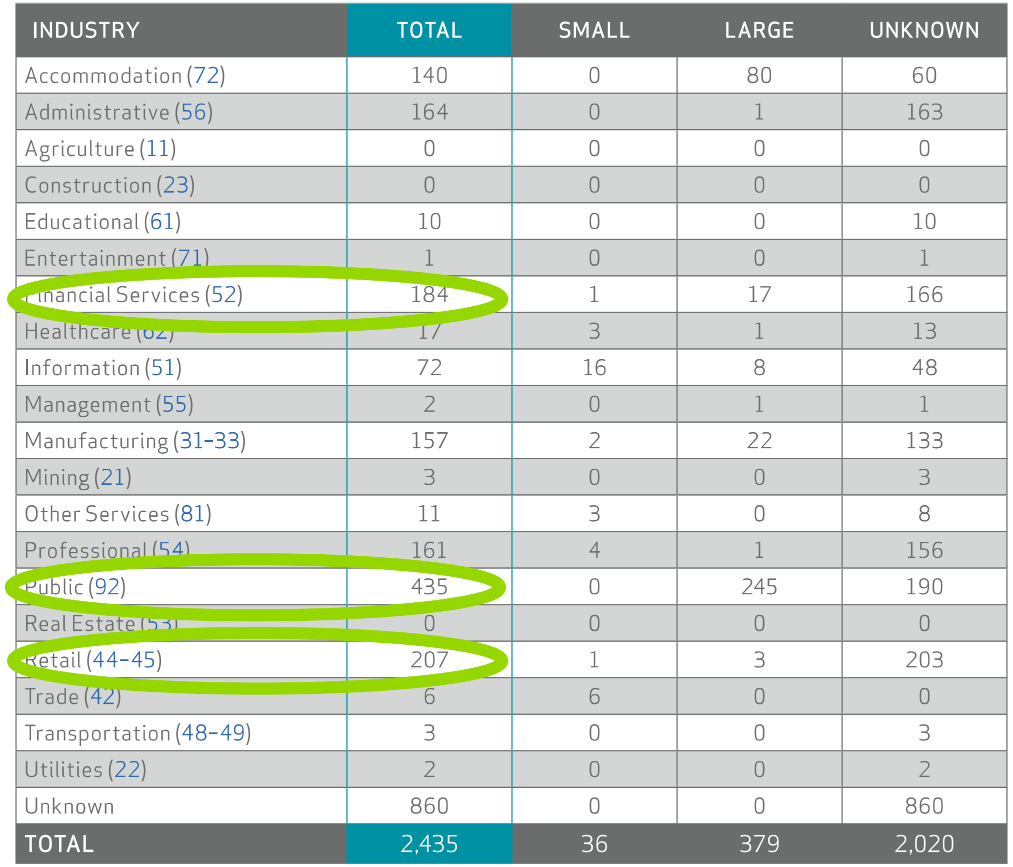


DDoS Attacks Exposure



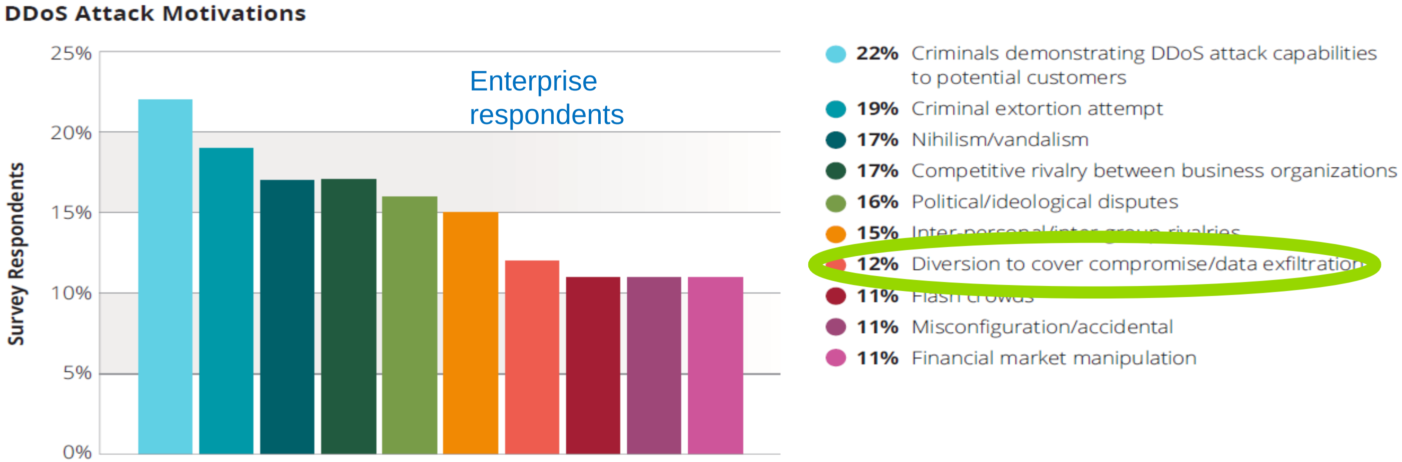
- **Any organization can be the target of a DDoS attack**
- **Most affected industries: Public, Retail, and Financial Services ****
- ***Picture: Number of DDoS attacks by victim industry and organization size (small is < 1,000 employees) *****

***Source Verizon 2015 DBIR*

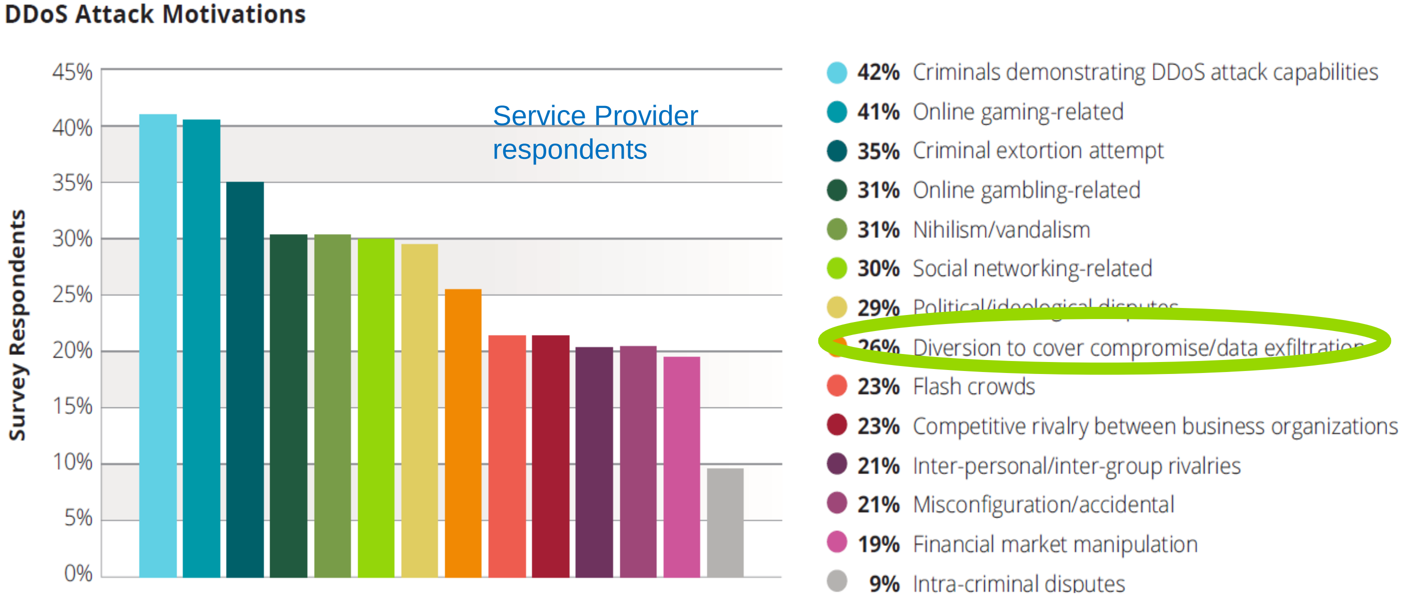


INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	140	0	80	60
Administrative (56)	164	0	1	163
Agriculture (11)	0	0	0	0
Construction (23)	0	0	0	0
Educational (61)	10	0	0	10
Entertainment (71)	1	0	0	1
Financial Services (52)	184	1	17	166
Healthcare (62)	17	3	1	13
Information (51)	72	16	8	48
Management (55)	2	0	1	1
Manufacturing (31-33)	157	2	22	133
Mining (21)	3	0	0	3
Other Services (81)	11	3	0	8
Professional (54)	161	4	1	156
Public (92)	435	0	245	190
Real Estate (53)	0	0	0	0
Retail (44-45)	207	1	3	203
Trade (42)	6	6	0	0
Transportation (48-49)	3	0	0	3
Utilities (22)	2	0	0	2
Unknown	860	0	0	860
TOTAL	2,435	36	379	2,020

DDoS Attacks Motivations

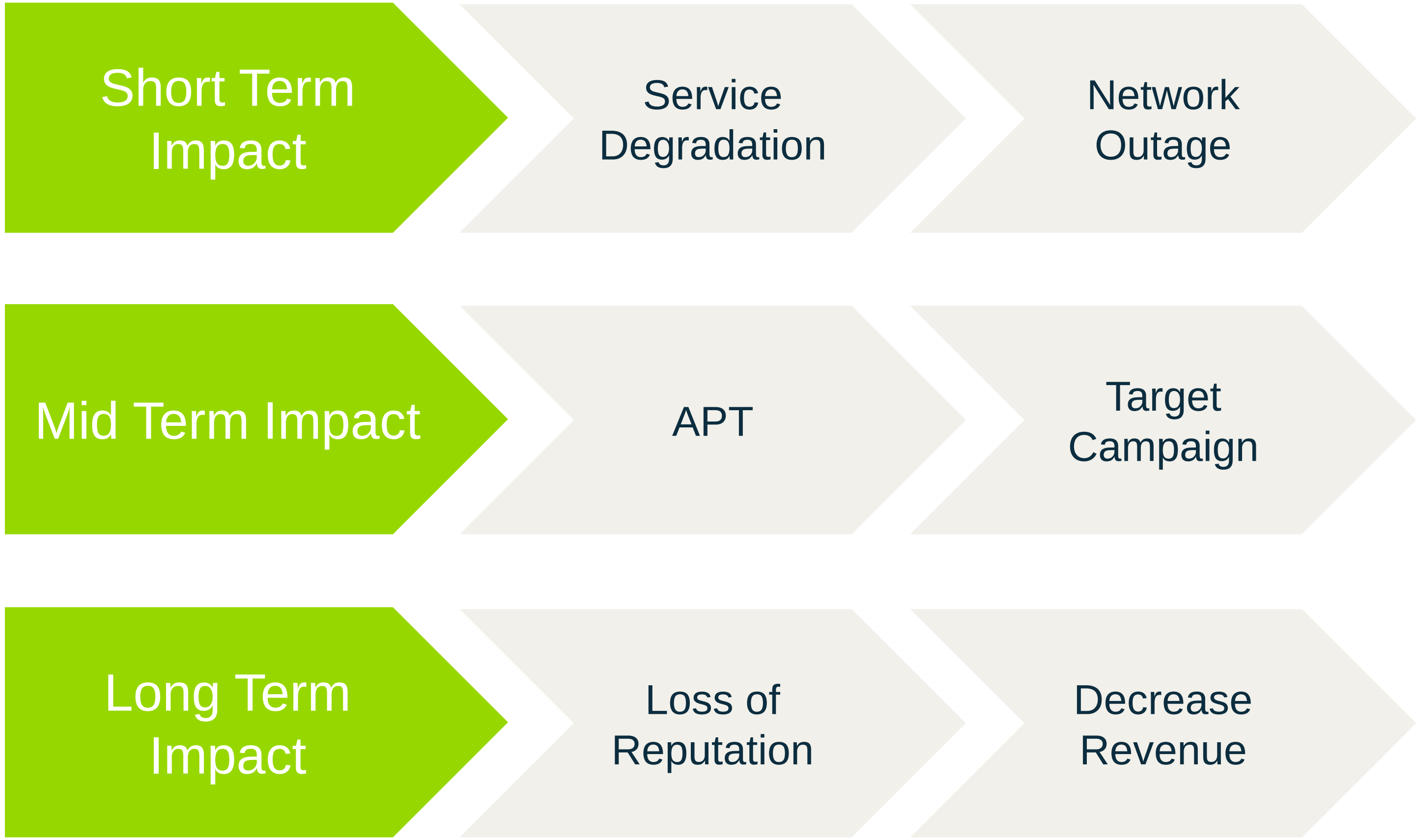

DDoS Attack Motivations

Enterprise respondents


DDoS Attack Motivations

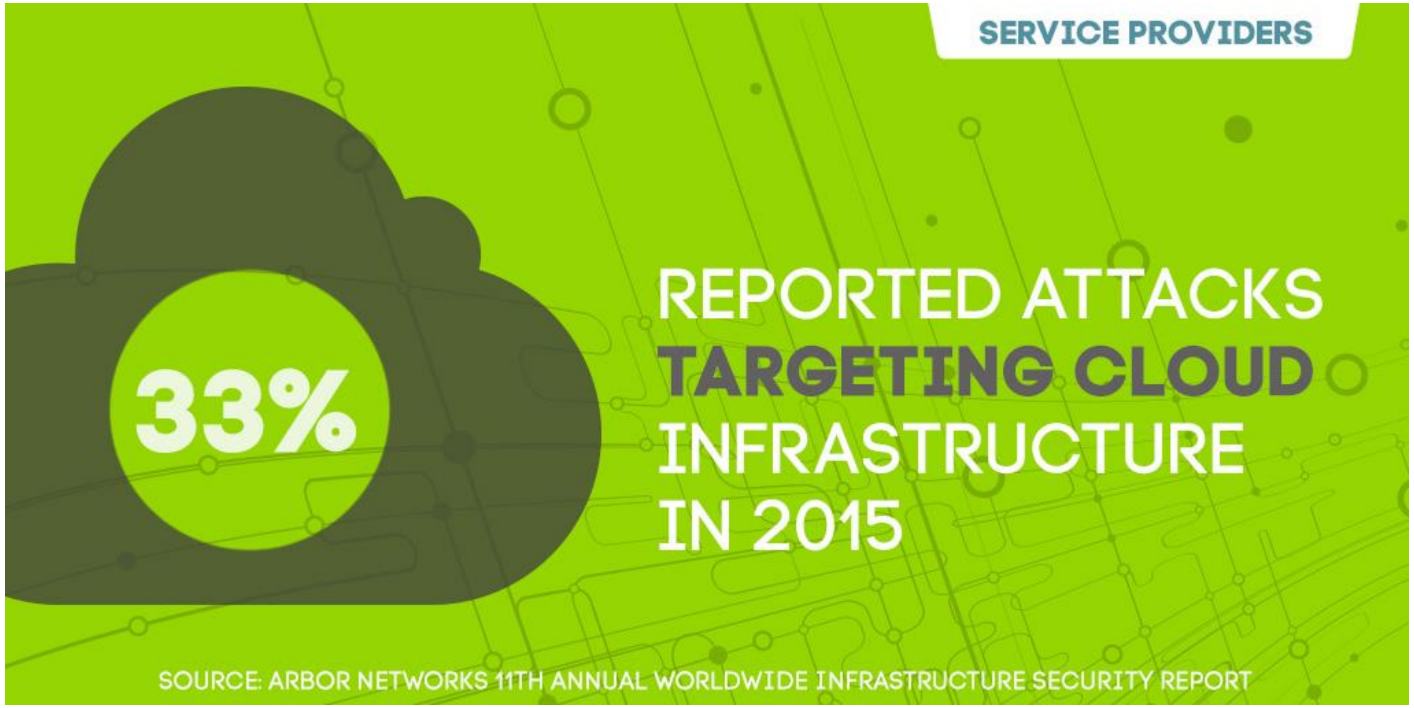
Service Provider respondents

DDoS Attacks Impacts



Short Term Impact	Service Degradation	Network Outage
Mid Term Impact	APT	Target Campaign
Long Term Impact	Loss of Reputation	Decrease Revenue

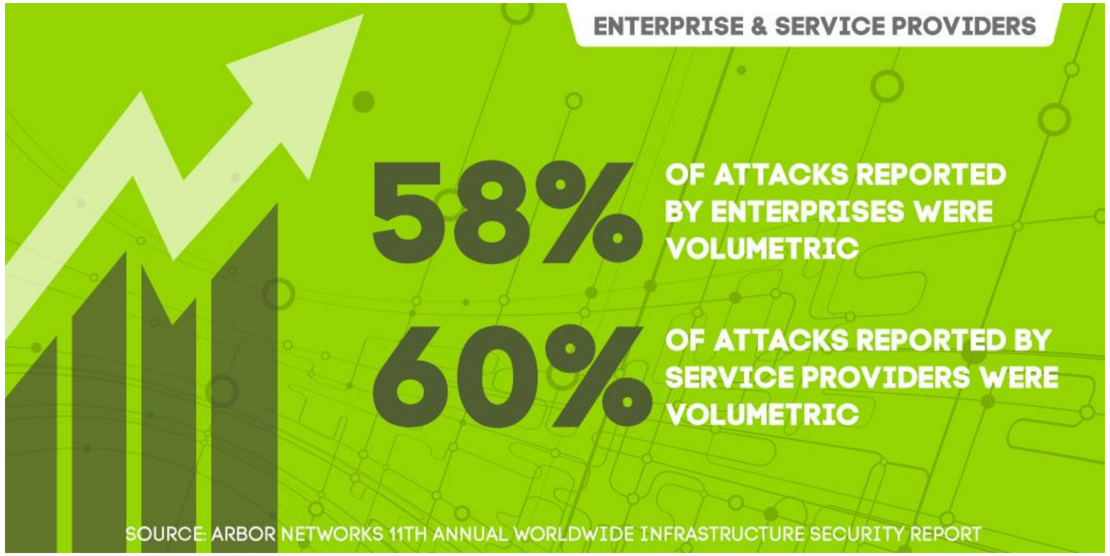
DDoS and the move to Cloud


SERVICE PROVIDERS
33%
REPORTED ATTACKS
TARGETING CLOUD
INFRASTRUCTURE
IN 2015
SOURCE: ARBOR NETWORKS 11TH ANNUAL WORLDWIDE INFRASTRUCTURE SECURITY REPORT

- **Global cloud IP traffic will almost quadruple (3.7-fold) over the next 5 years. Overall, cloud IP traffic will grow at a CAGR of 30 percent from 2015 to 2020 ****

*** Source Cisco Global Cloud Index: Forecast and Methodology, 2015–2020*

DDoS Attacks to SP and the Enterprise

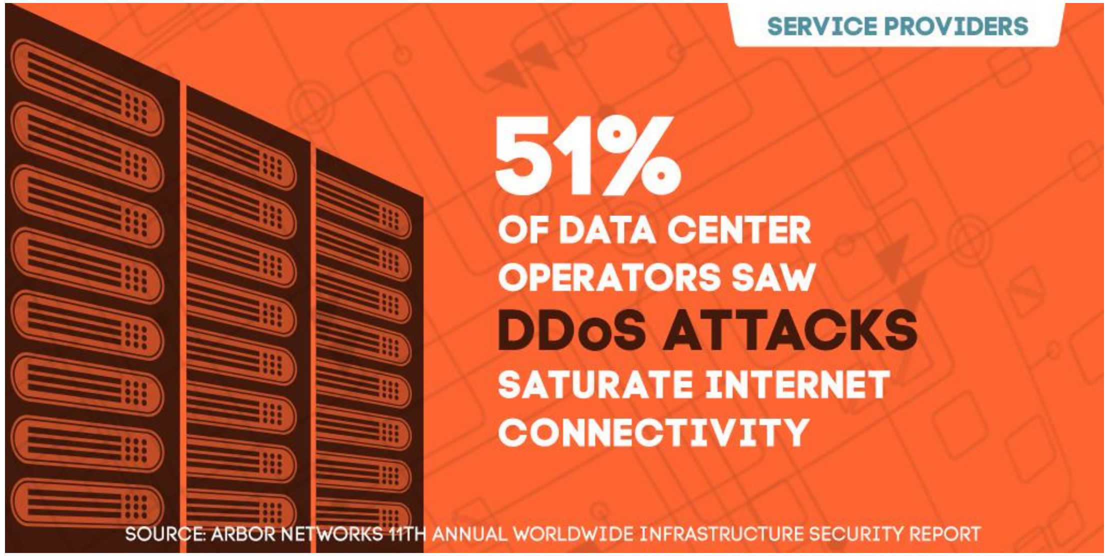


ENTERPRISE & SERVICE PROVIDERS

58% OF ATTACKS REPORTED BY ENTERPRISES WERE VOLUMETRIC

60% OF ATTACKS REPORTED BY SERVICE PROVIDERS WERE VOLUMETRIC

SOURCE: ARBOR NETWORKS 11TH ANNUAL WORLDWIDE INFRASTRUCTURE SECURITY REPORT

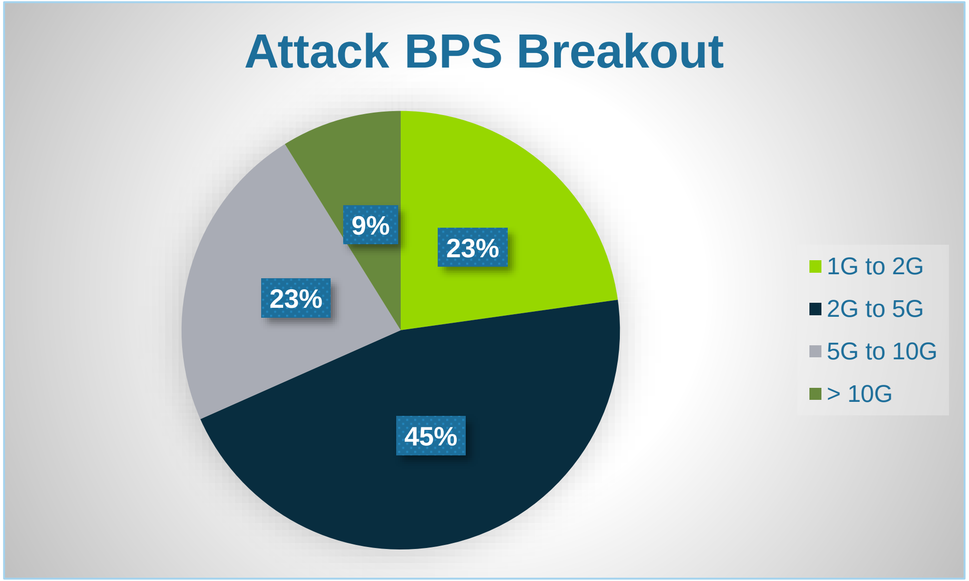


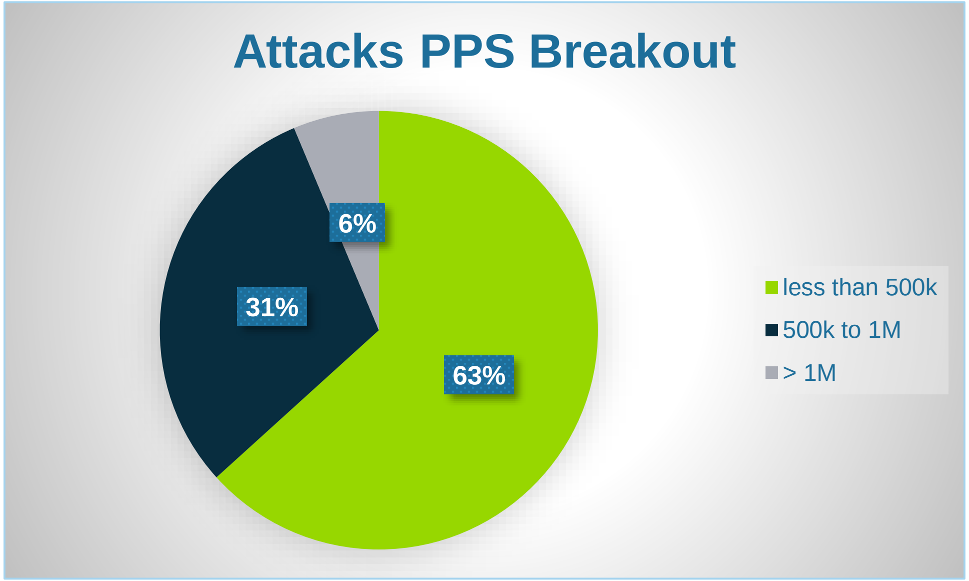
SERVICE PROVIDERS

51% OF DATA CENTER OPERATORS SAW DDoS ATTACKS SATURATE INTERNET CONNECTIVITY

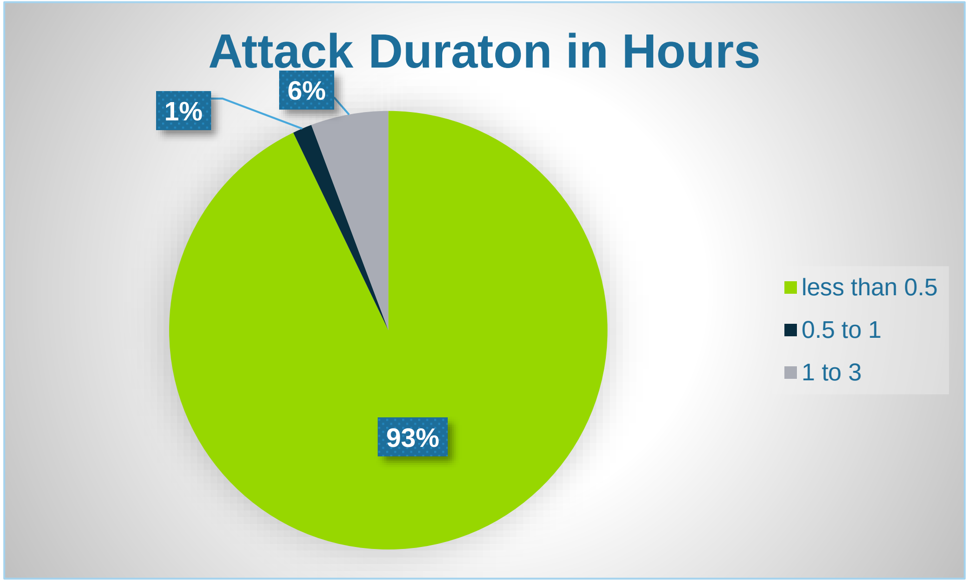
SOURCE: ARBOR NETWORKS 11TH ANNUAL WORLDWIDE INFRASTRUCTURE SECURITY REPORT

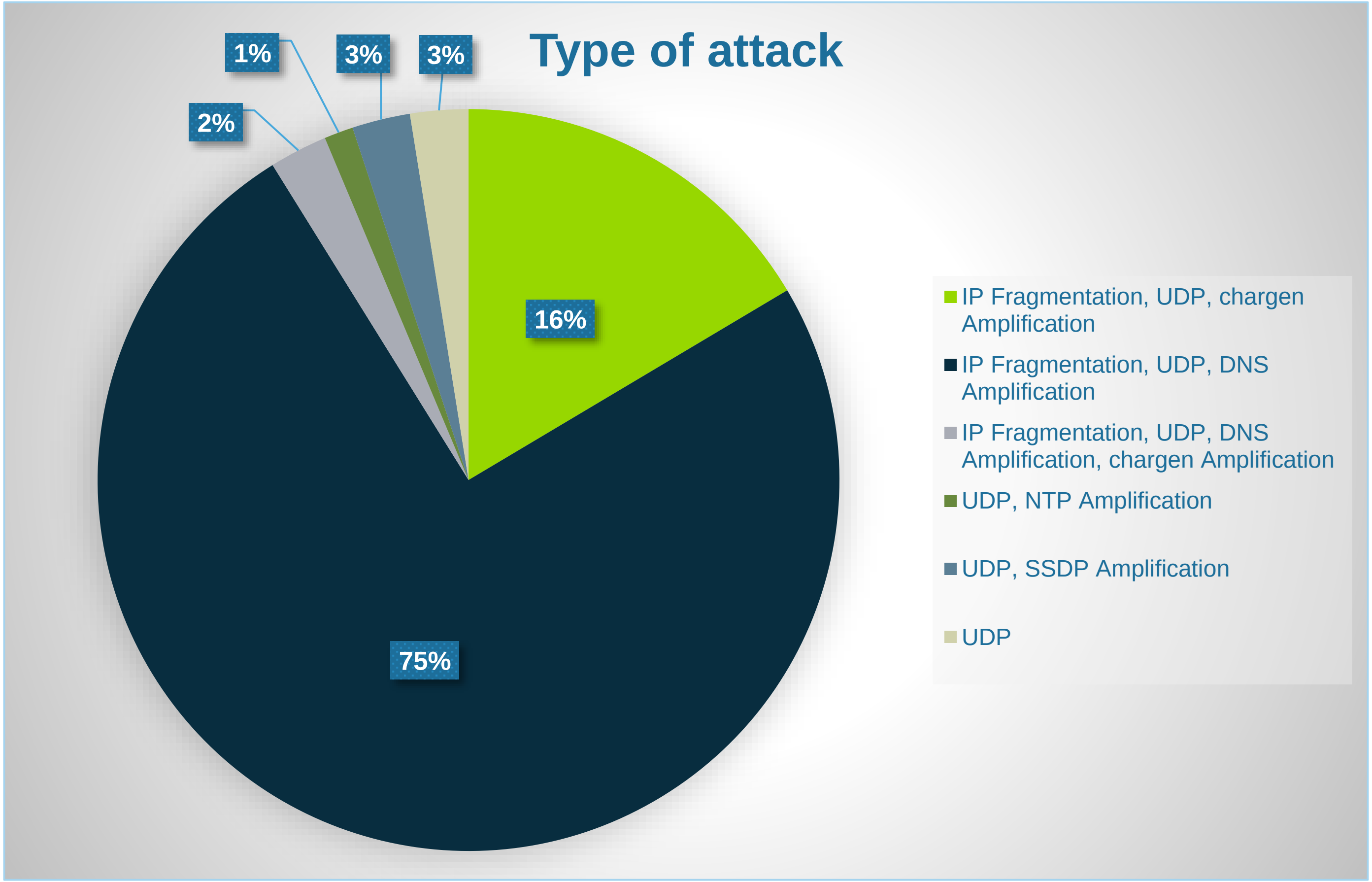
DDoS Attacks in Cyprus – 2016 Sample Arbor Data

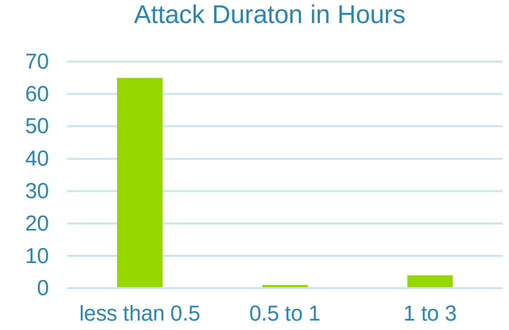




DDoS Attacks in Cyprus – 2016 Sample Arbor Data

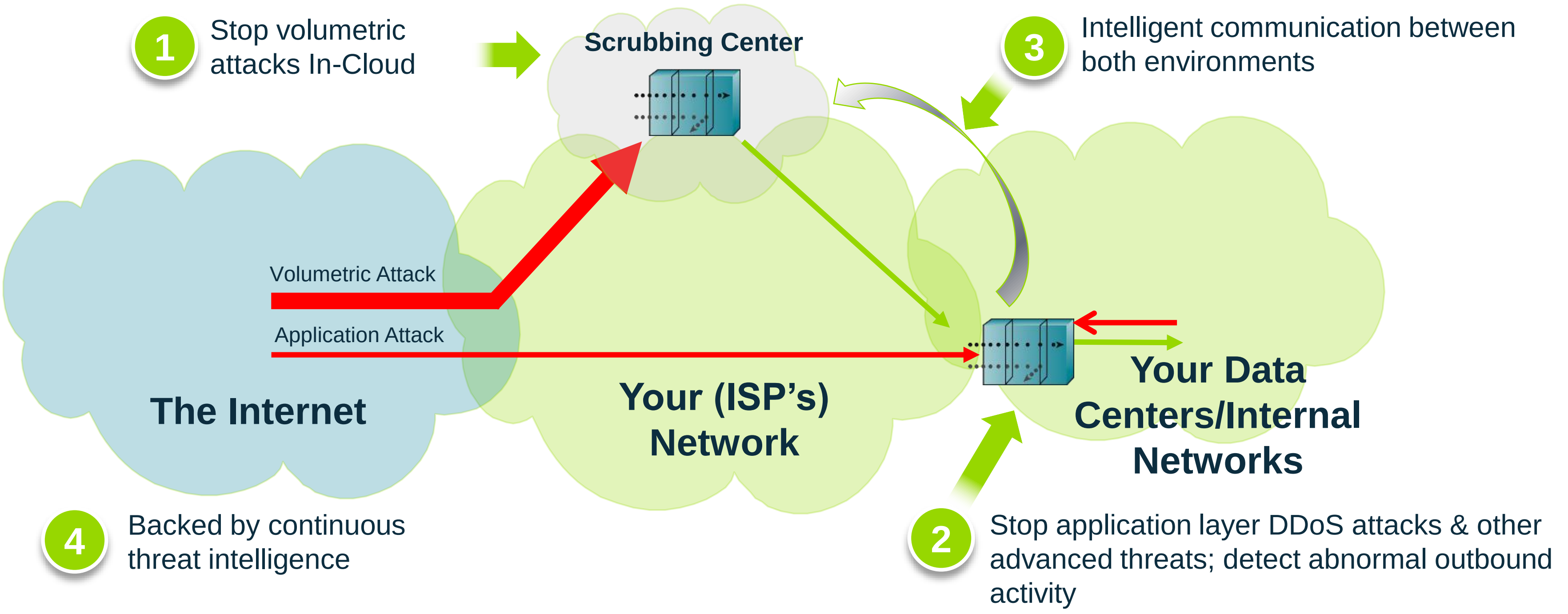






Stopping DDoS Attacks

Layered DDoS Attack Protection


1
Stop volumetric attacks In-Cloud
Scrubbing Center
3
Intelligent communication between both environments
Volumetric Attack
Application Attack
The Internet
Your (ISP's) Network
Your Data Centers/Internal Networks
4
Backed by continuous threat intelligence
2
Stop application layer DDoS attacks & other advanced threats; detect abnormal outbound activity

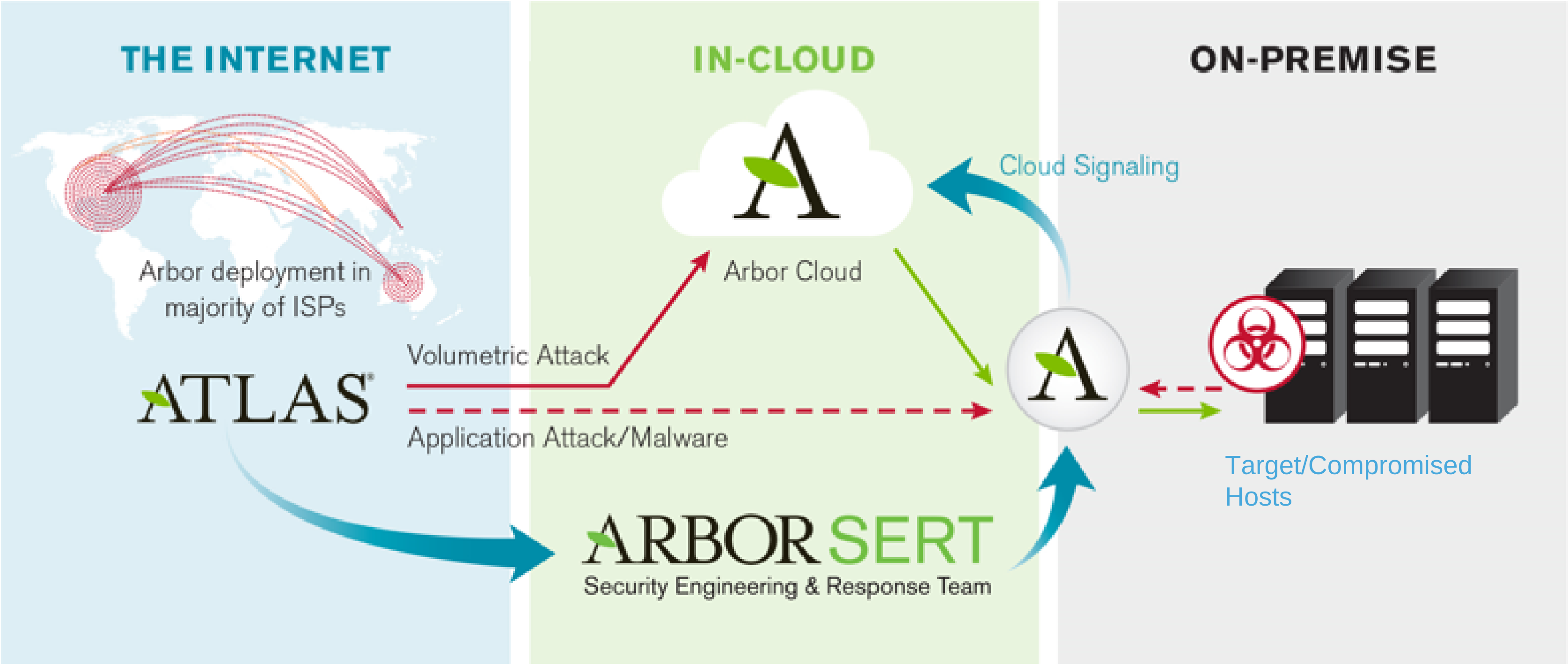
Backed by Continuous Threat Intelligence

A Recommended Industry Best Practice:

FORRESTER® IDC FROST & SULLIVAN Infonetics RESEARCH Securosis ovum

Arbor’s DDoS Protection Solution

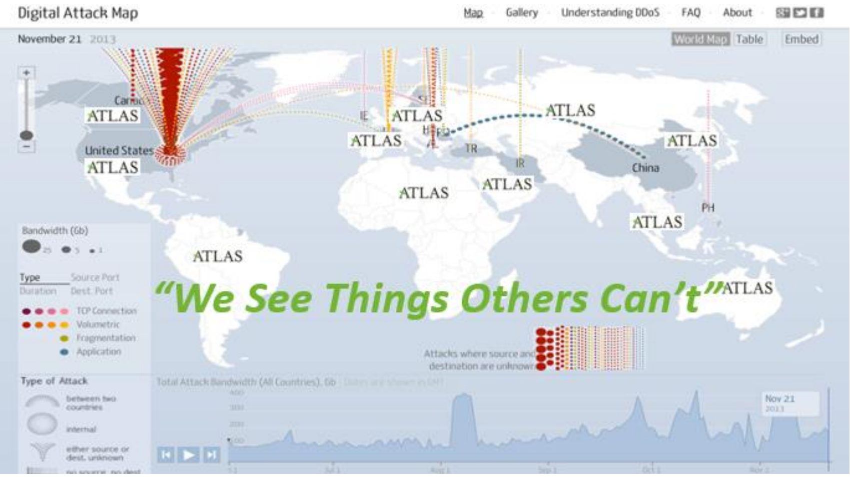
Comprehensive DDoS Protection Products & Services



Armed with Global Visibility & Actionable Threat Intelligence

The Internet – Atlas and ASERT

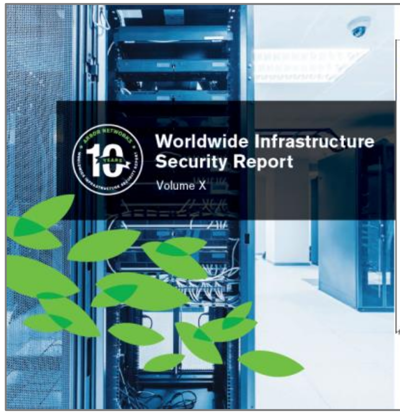
- 15 years of deployment in a majority of world’s ISPs offer unique visibility into global threats
- Over 300 ISPs participating in ATLAS; providing Global Visibility and Threat Intelligence
- ASERT is a team of industry experts who conduct threat research, help customer mitigate DDoS attacks and create ATLAS Intelligence Feeds
- ATLAS & ASERT continuously arm all Arbor products and services with global threat intelligence ATLAS Intelligence Feed allowing customers to stay abreast of DDoS and advanced threats

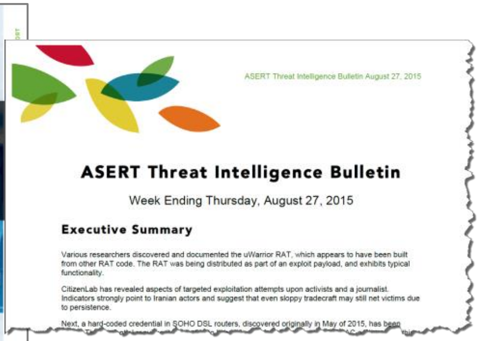


ARBOR SERT
Security Engineering & Response Team

ATLAS

AIF




ASERT Threat Intelligence Bulletin August 27, 2015

ASERT Threat Intelligence Bulletin

Week Ending Thursday, August 27, 2015

Executive Summary

Various researchers discovered and documented the uWarrior RAT, which appears to have been built from other RAT code. The RAT was being distributed as part of an exploit payload, and exhibits typical functionality.

CitizenLab has revealed aspects of targeted exploitation attempts upon activists and a journalist. Indicators strongly point to Iranian actors and suggest that even sloppy tradecraft may still net victims due to persistence.

Next, a hard-coded credential in SOHO DSL routers, discovered originally in May of 2015, has been

Conclusion

- **DDoS Attacks may bring down any Service**
- **Direct impact as loss of revenues, lower customers experience**

- **Arbor Networks' Solution guarantees Protection by:**
  - **Continuous traffic analysis and visibility: ATLAS, Digital Attack Map**
  - **AIF, ASERT network trend and application analysis**
  - **Automated Workflow for Mitigating all attacks on premises and cloud**
  - **Detection and Mitigation of full scope DDoS Attacks with High Accuracy**
  - **Shortest time to protect**

Thank You

abulletti@arbor.net
+39 3388661617

ARBOR NETWORKS
The Security Division of NETSCOUT