Akamai

Cybersecurity: trend emergenti a livello globale

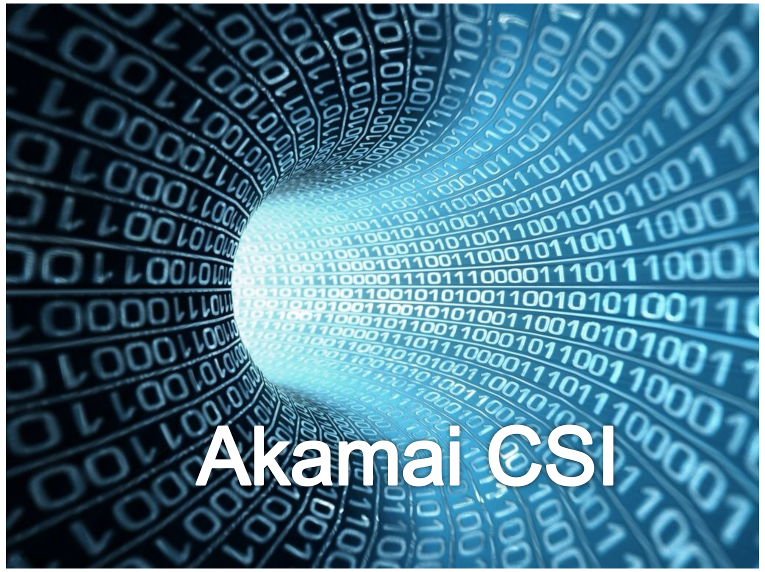
L’intelligence come strumento di prevenzione e contrasto

Alessandro Livrea- Country Manager- Akamai Italia

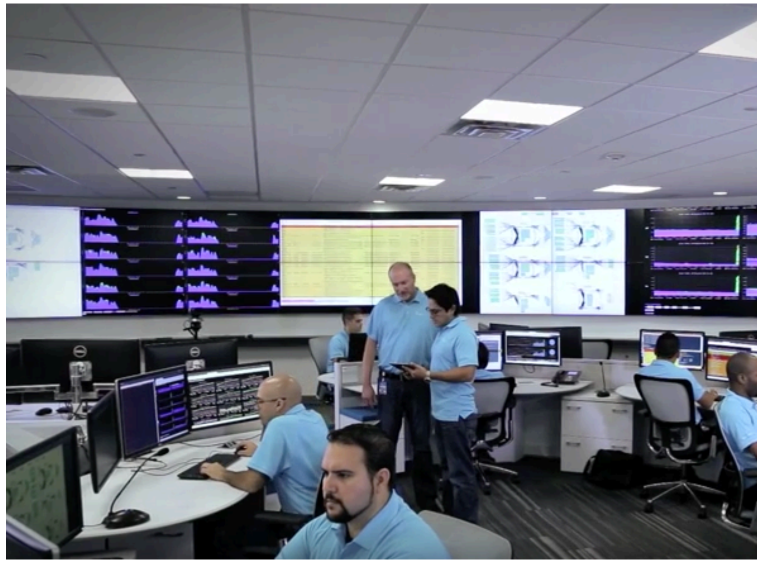
Una piattaforma Globale

216,000+ servers
1,500+ networks
120+ paesi
3,300 locations

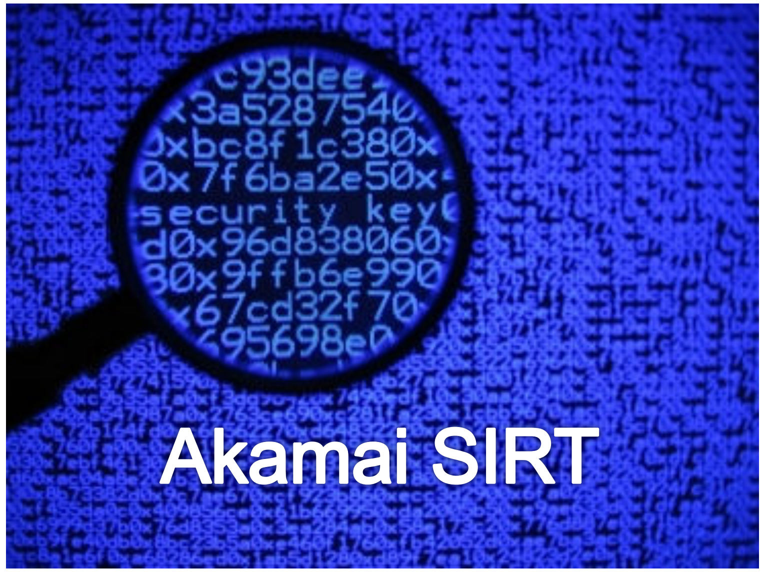
Da dove arrivano i dati che vedremo?



Kona WAF
Web Application Attacks
Machine Generated



Prolexic Routed
SOC
Human



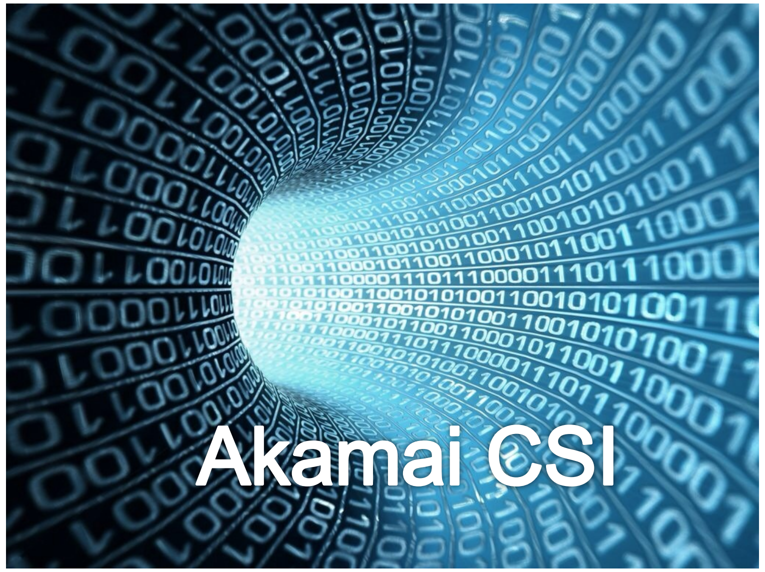
2000 miliardi di Hits al giorno

1 Miliardo di IP a trimestre

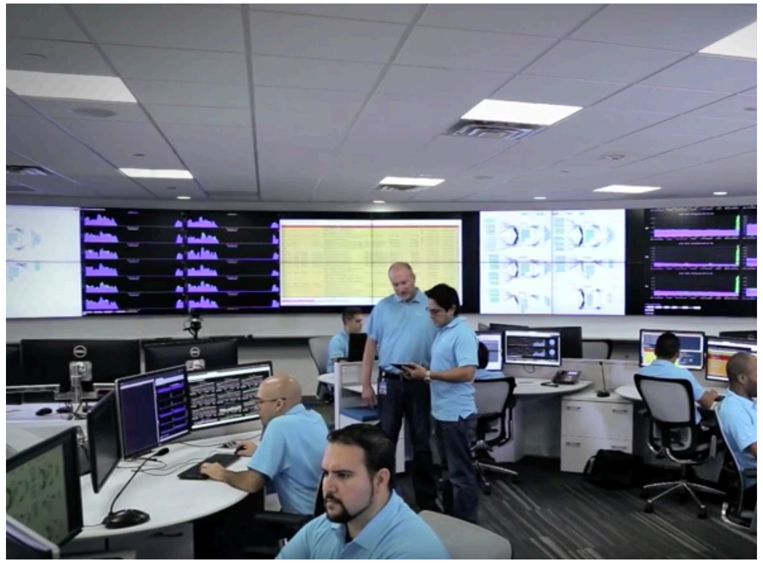
Oltre 2 Petabytes di dati inerenti la sicurezza

20 Terabytes di dati al giorno su attacchi

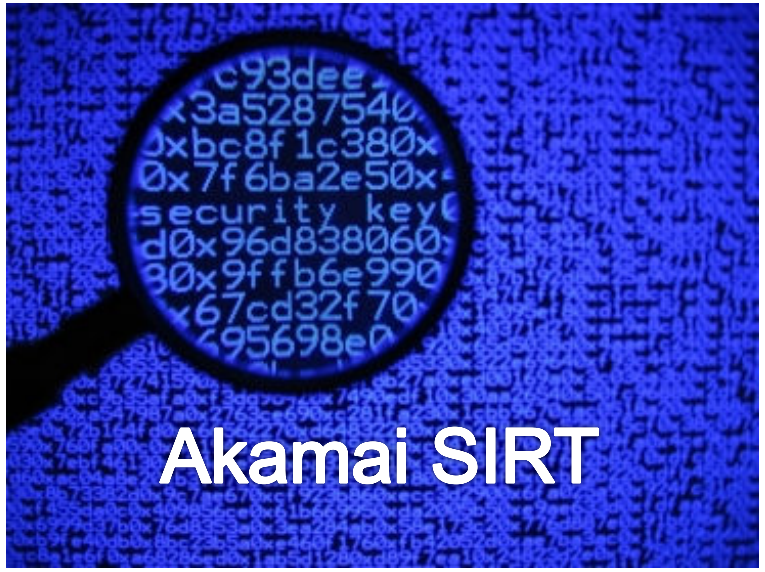
Da dove arrivano i dati che vedremo?



Kona WAF
Web Application Attacks
Machine Generated



Prolexic Routed
SOC
Human



9 Common Web Attack Vectors

SQLi / SQL injection: User content is passed to an SQL statement without proper validation

LFI / Local file inclusion: Gains unauthorized read access to local files on the web server

RFI / Remote file inclusion: Abuse of the dynamic file include mechanism available in many programming languages to load remote malicious code into the victim web application

PHPi / PHP injection: Injects PHP code that gets executed by the PHP interpreter

CMDi / Command injection: Executes arbitrary shell commands on the target system

JAVAi / Java injection: Abuses the Object Graph Navigation Language (OGNL), a Java expression language. Popular due to recent flaws in the Java-based Struts Framework, which uses OGNL extensively

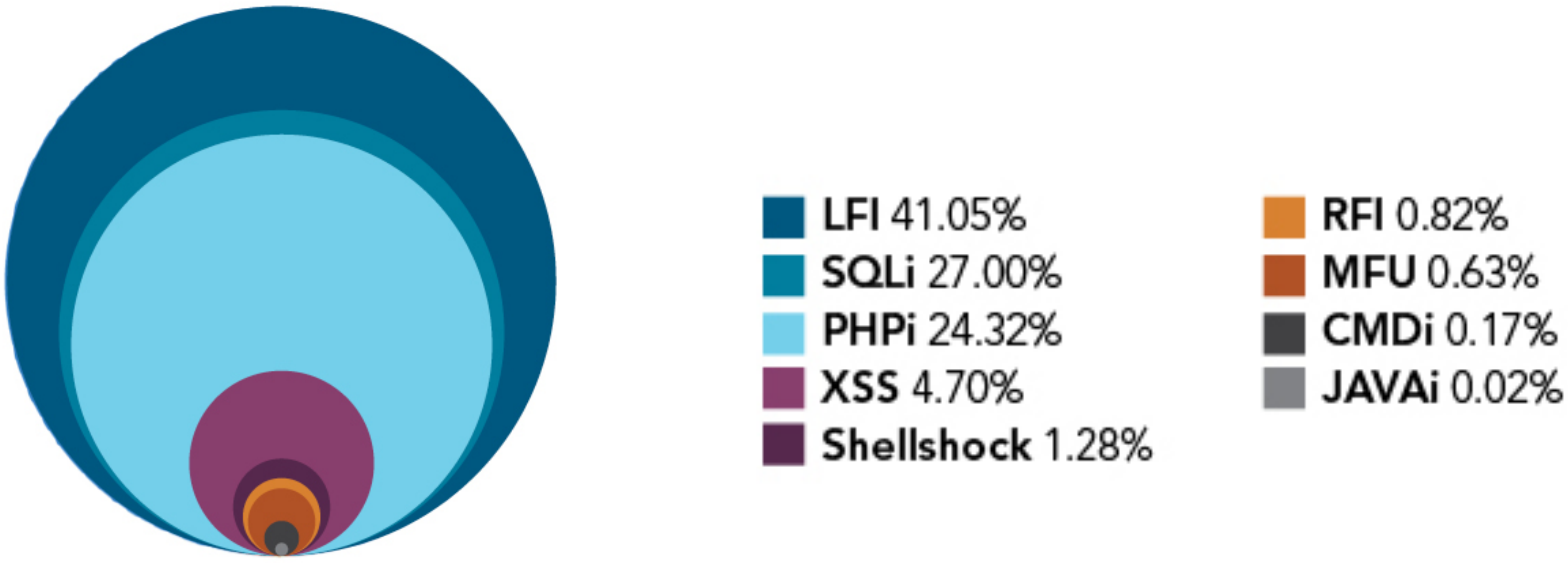
MFU / Malicious file upload (or unrestricted file upload): Uploads unauthorized files to the target application that may be used later to gain full control over the system

XSS / Cross-site scripting: Injects client-side code into web pages viewed by others whose browsers execute the code within the security context (or zone) of the hosting web site. Reads, modifies and/or transmits data accessible by the browser

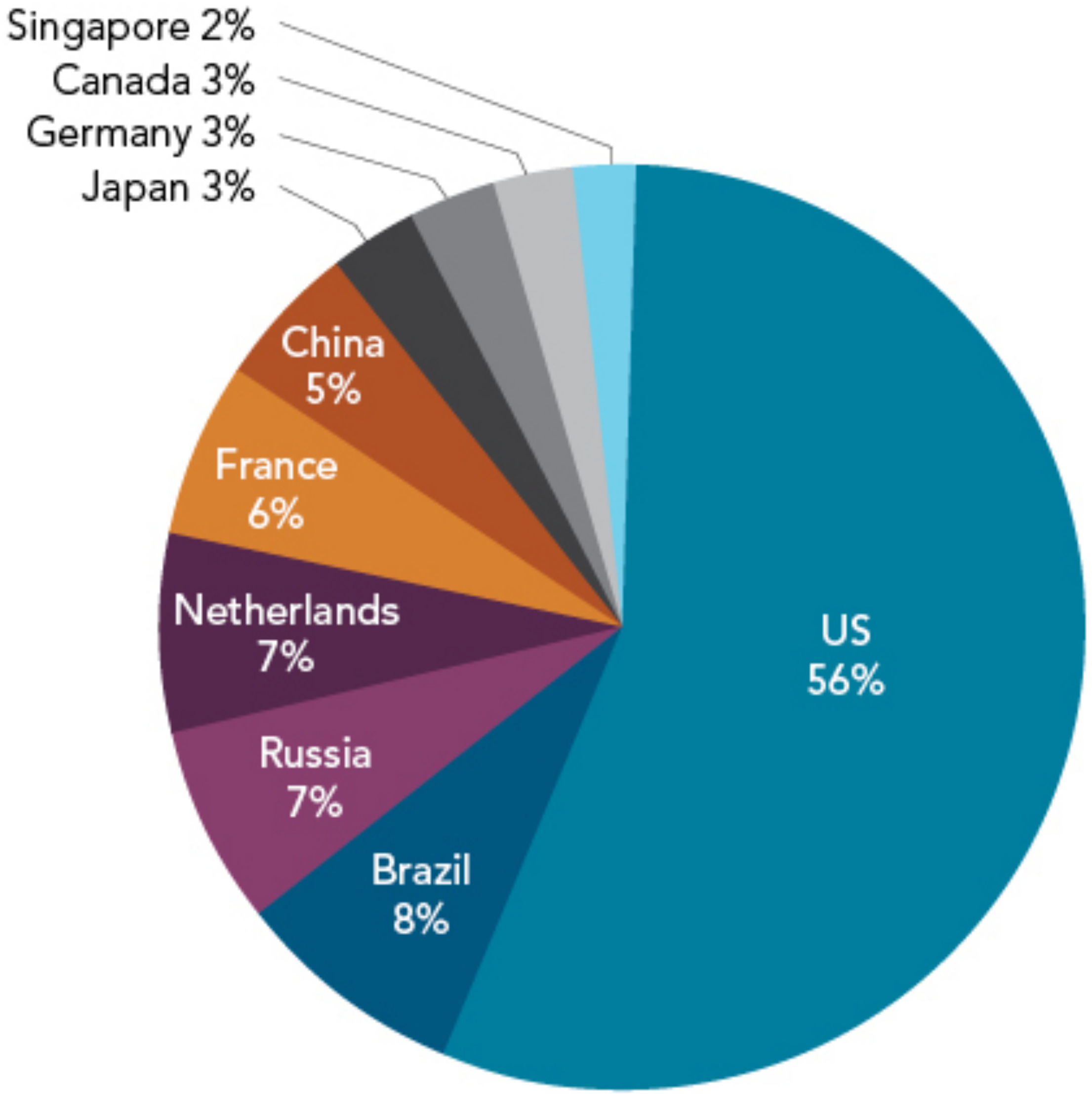
Shellshock **/** Disclosed in September 2014: A vulnerability in the Bash shell (the default shell for Linux and mac OS X) that allows for arbitrary command execution by a remote attacker

Attacchi applicativi rispetto al Q3 2015

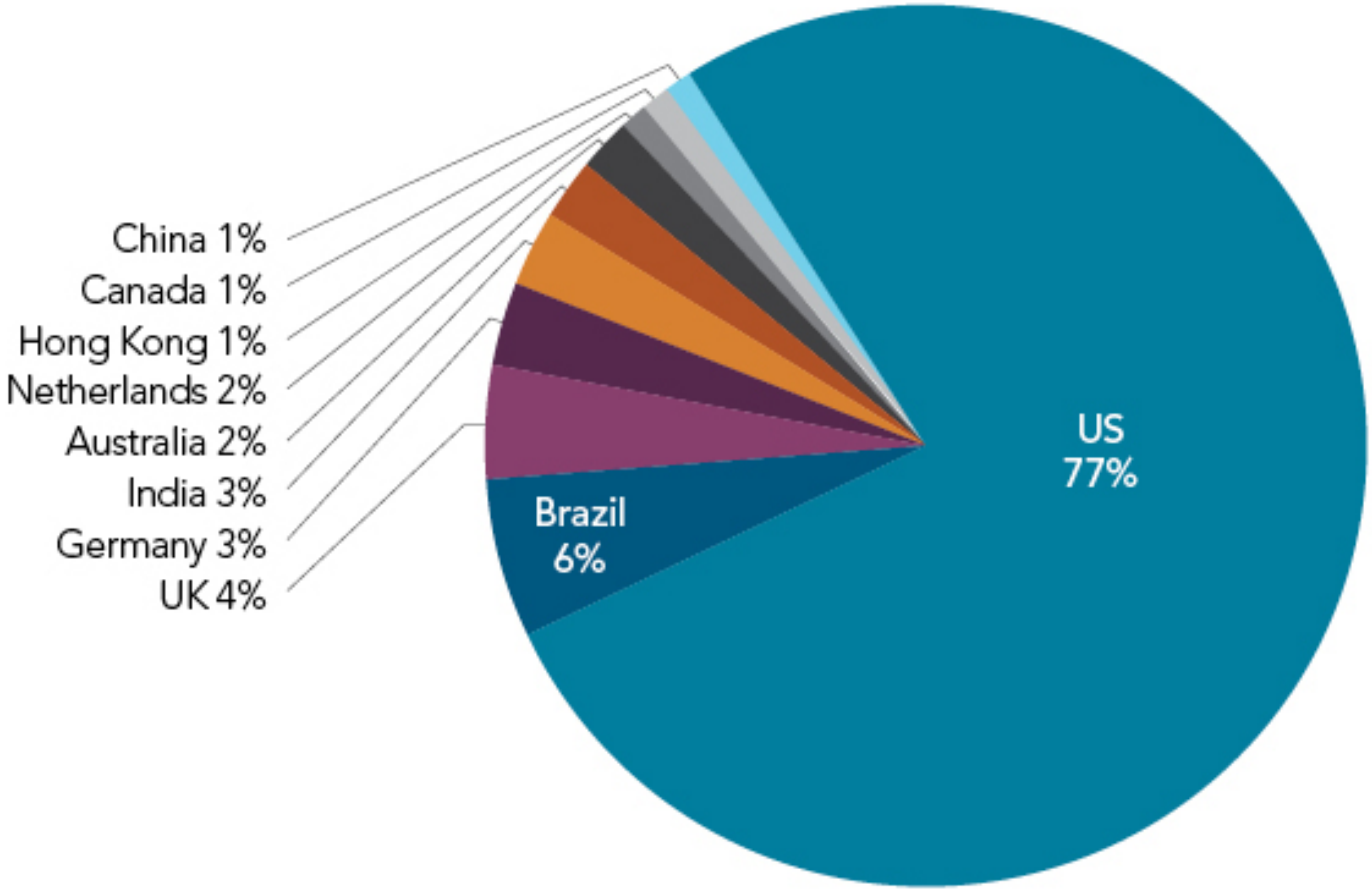
- 28 % ↑ Attacchi di tipo applicativo
- 28% ↑ Attacchi su protocollo HTTP
- 24% ↑ Attacchi su protocollo HTTPS



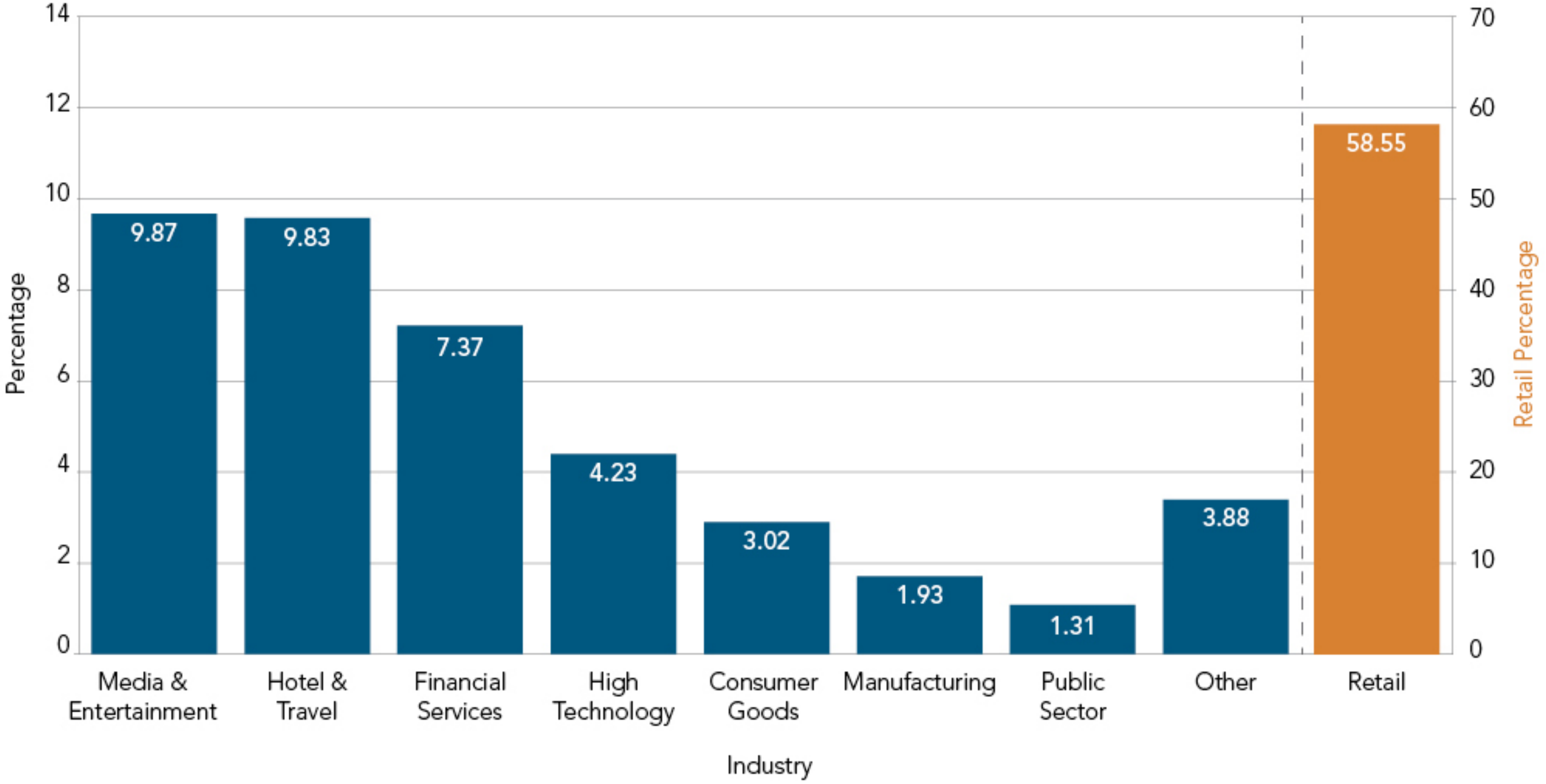
Principali fonti di attacco applicativo, Q4 2015



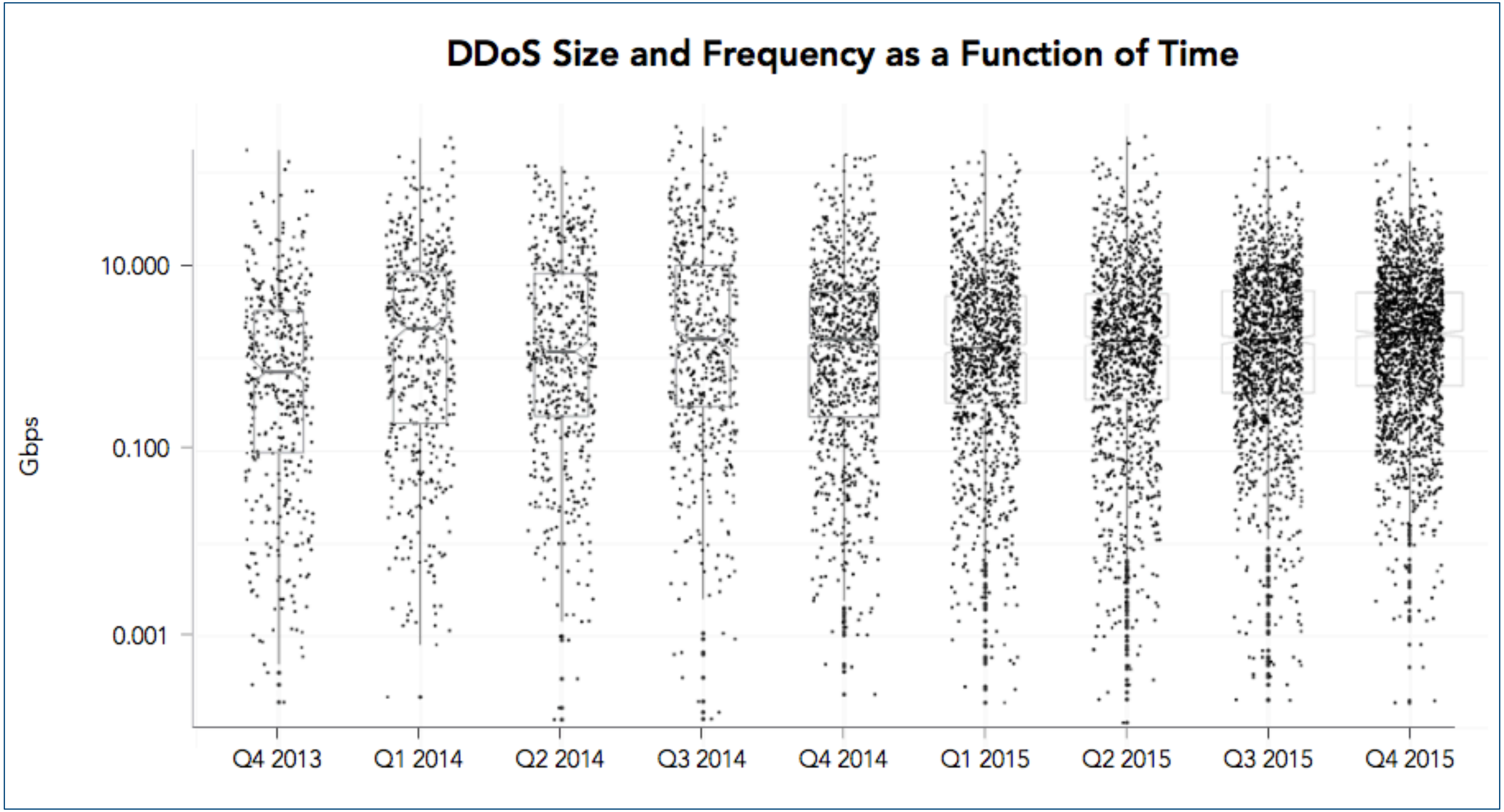
Top 10 Paesi Target, Q4 2015



Attacchi di tipo applicativo per Industry, Q4 2015



DDoS: Attacchi come mai prima



DDoS un fenomeno in evoluzione

Single attacker

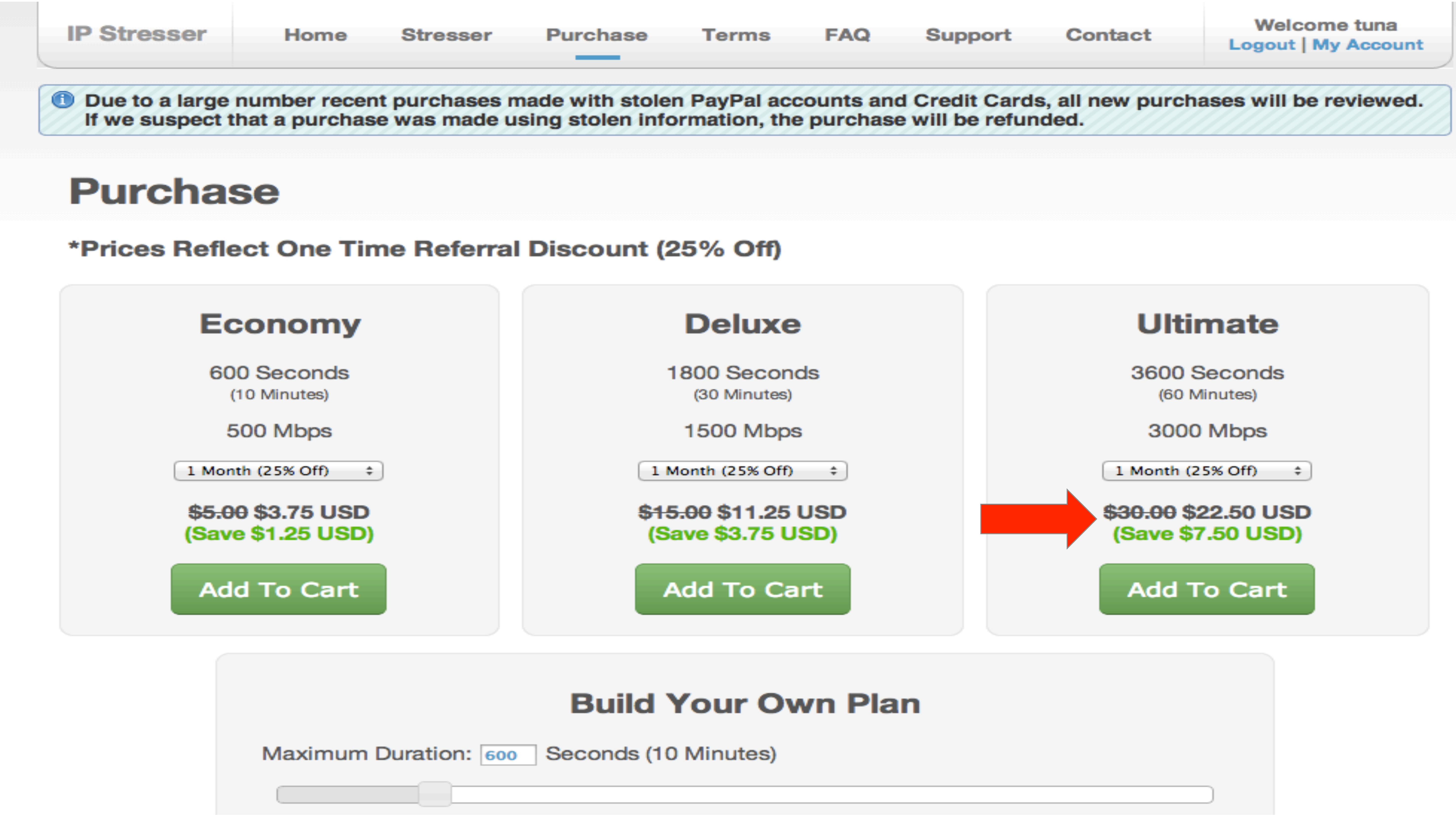
Botnet (PC and servers infected by malware)

Reflection attacks

- Increase in attack volume

Booter / Stresser

- Low cost and simple payment options
- “Stress test”



Due to a large number recent purchases made with stolen PayPal accounts and Credit Cards, all new purchases will be reviewed. If we suspect that a purchase was made using stolen information, the purchase will be refunded.

Purchase

***Prices Reflect One Time Referral Discount (25% Off)**

Economy

600 Seconds
(10 Minutes)

500 Mbps

1 Month (25% Off)

~~$5.00~~ $3.75 USD
(Save $1.25 USD)

Deluxe

1800 Seconds
(30 Minutes)

1500 Mbps

1 Month (25% Off)

~~$15.00~~ $11.25 USD
(Save $3.75 USD)

Ultimate

3600 Seconds
(60 Minutes)

3000 Mbps

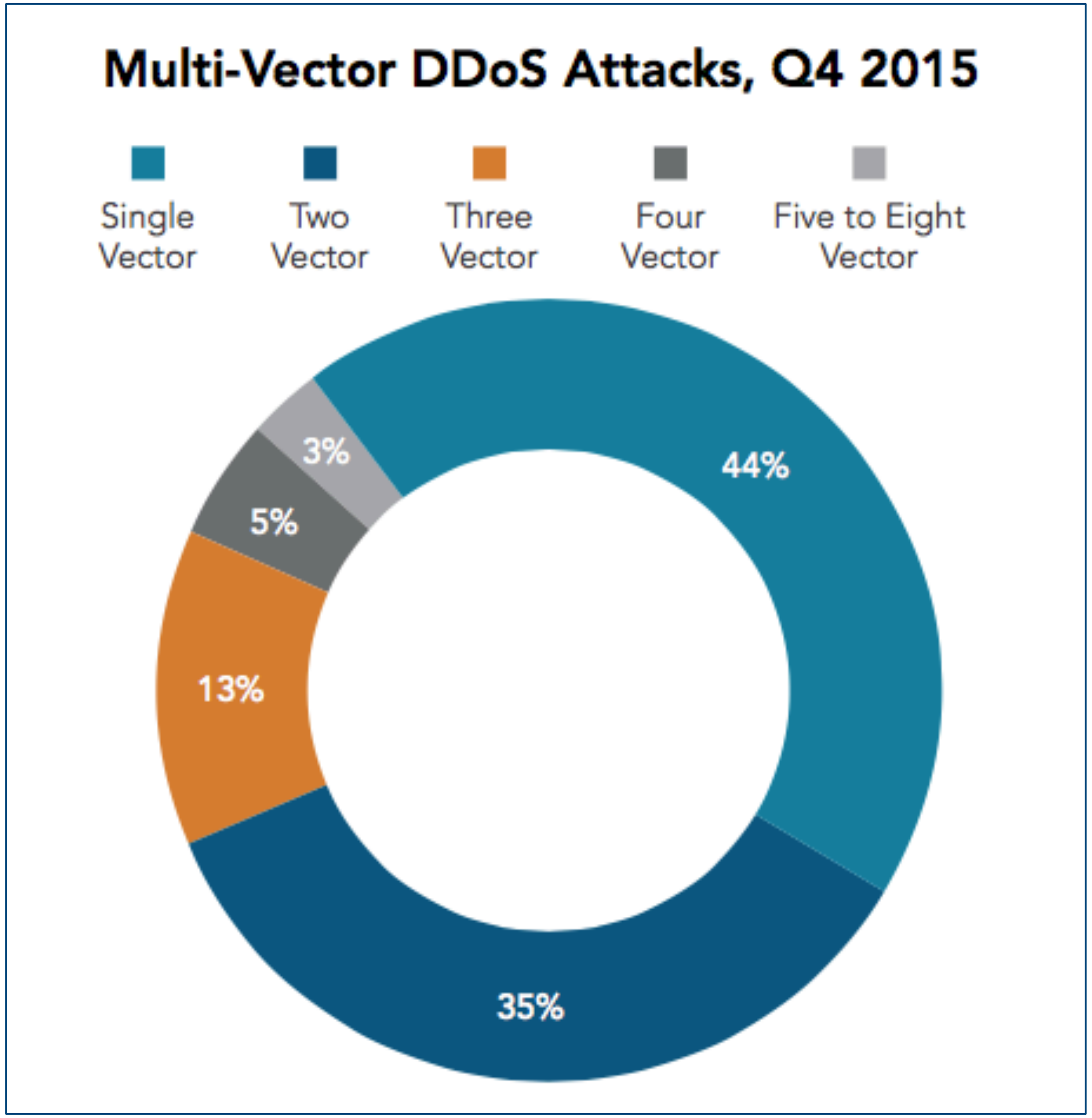
1 Month (25% Off)

~~$30.00~~ $22.50 USD
(Save $7.50 USD)

Build Your Own Plan

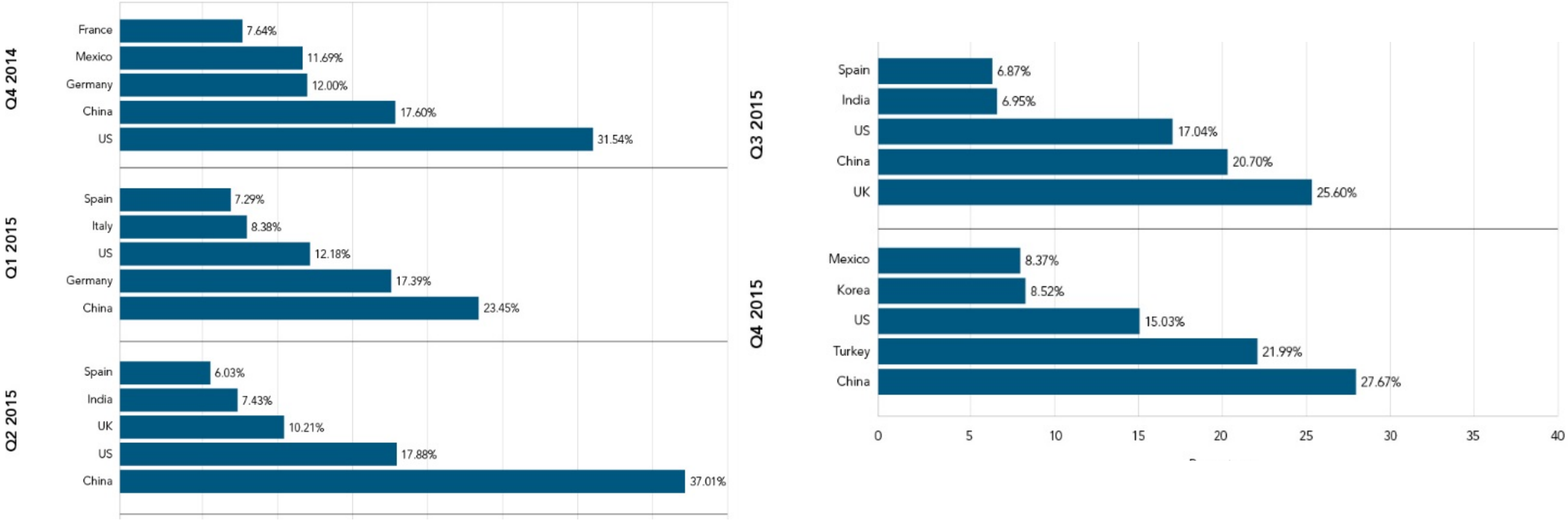
Maximum Duration: 600 Seconds (10 Minutes)

Booter-Stresser come strumenti di attacco multivettoriale



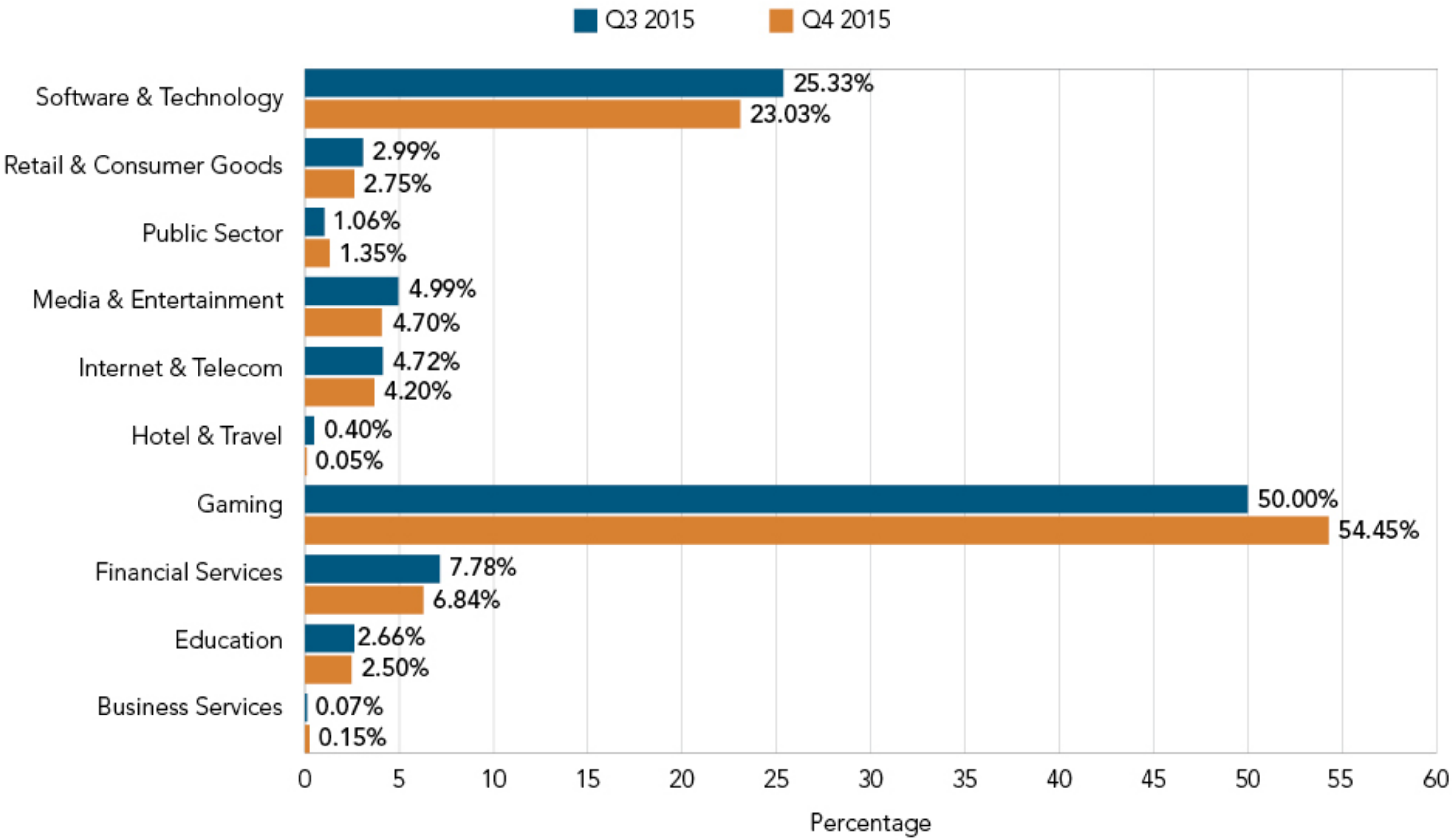
Multi-Vector DDoS Attacks, Q4 2015

Top 5 Paesi fonte di attacchi DDoS, Q4 2014 - Q4 2015

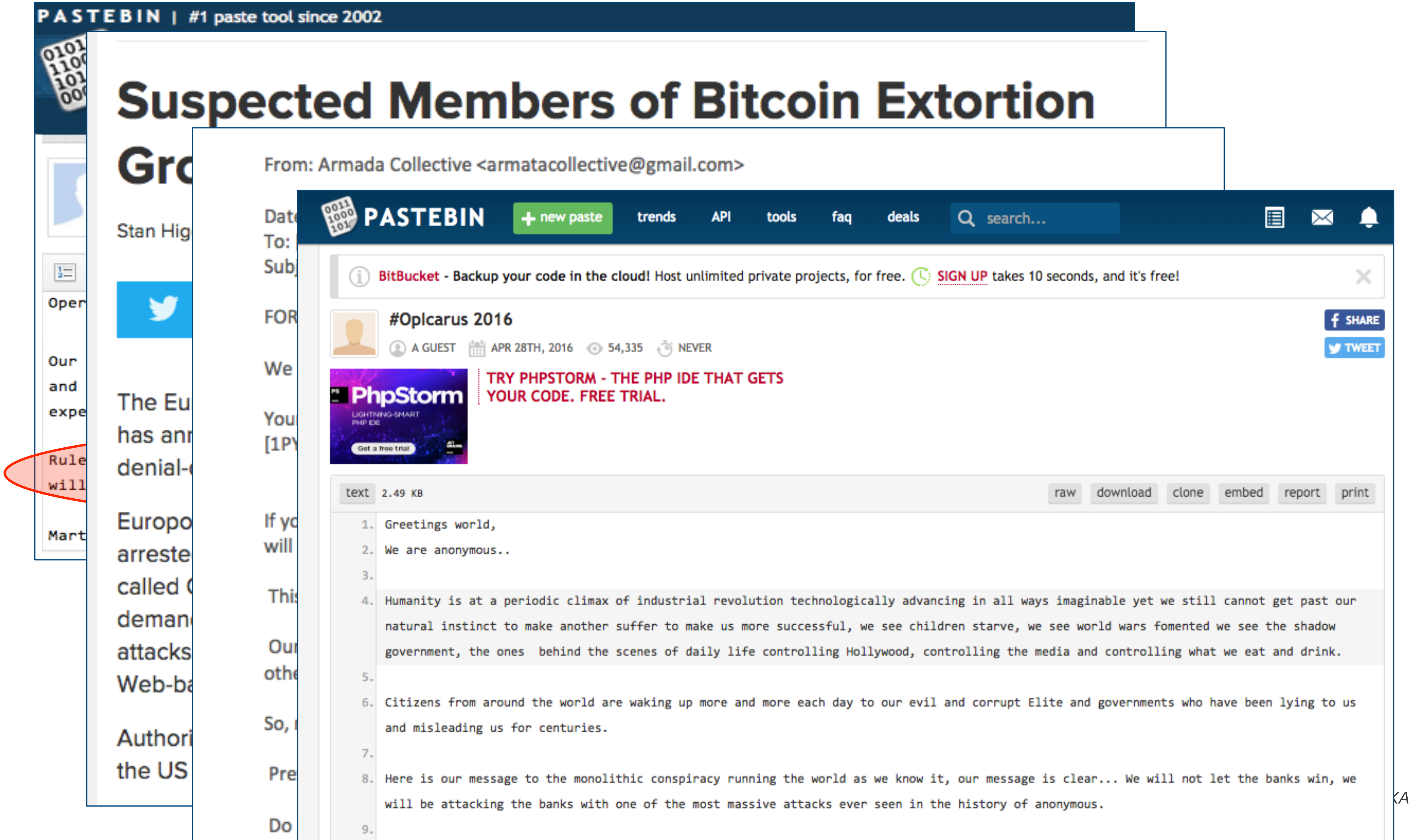


USA e China sono state le principali fonti di attacco per 5 trimestri ma…

Frequenza attacchi DDoS per Industry



Istituzioni finaziarie costantemente sotto attacco



Suspected Members of Bitcoin Extortion Gro

Stan Hig

The Eu has anr denial-

Europo arreste called demand attacks Web-ba

Authori the US

From: Armada Collective <armatacollective@gmail.com>

Dat
To:
Sub

FOR

We

You [1PY

If yo will

This

Our othe

So,

Pre

Do

#OpIcarus 2016

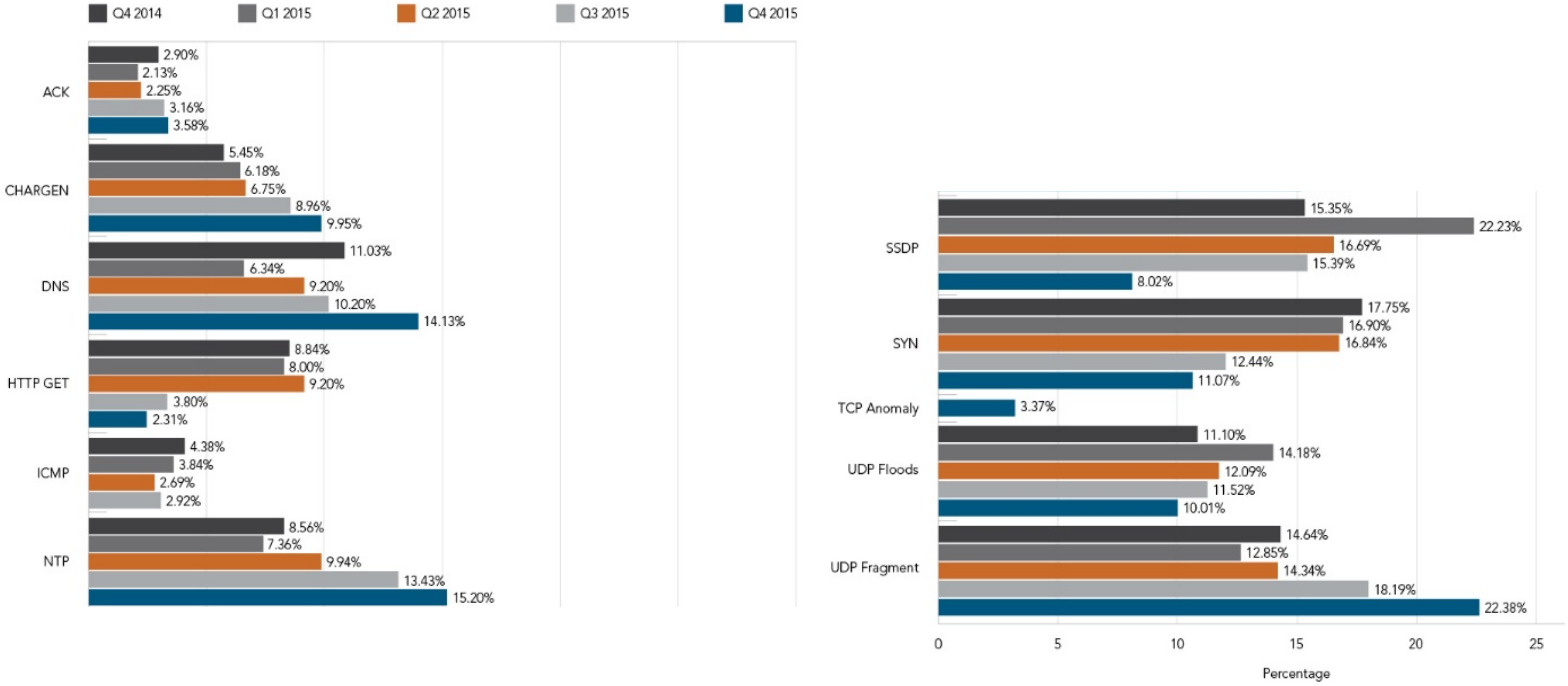
A GUEST APR 28TH, 2016 54,335 NEVER

```
Greetings world,
We are anonymous..

Humanity is at a periodic climax of industrial revolution technologically advancing in all ways imaginable yet we still cannot get past our natural instinct to make another suffer to make us more successful, we see children starve, we see world wars fomented we see the shadow government, the ones  behind the scenes of daily life controlling Hollywood, controlling the media and controlling what we eat and drink.

Citizens from around the world are waking up more and more each day to our evil and corrupt Elite and governments who have been lying to us and misleading us for centuries.

Here is our message to the monolithic conspiracy running the world as we know it, our message is clear... We will not let the banks win, we will be attacking the banks with one of the most massive attacks ever seen in the history of anonymous.
```

Cosa ci riserva il futuro

- Un utilizzo sempre più intensivo di stresser e Booter
- Un numero maggiore di attacchi
- Attacchi multipli verso lo stesso target
- Attacchi multivettoriali
- Attacchi sempre più grandi
- Entro 3 anni e mezzo ci aspettiamo che un attacco DDoS di medie dimesioni possa generare 1,5 Tbps di traffico

10 Most Frequent Attack Vectors by Quarter



Grazie!