Security without sacrificing performance

Konrad Kaczanowski & Rafał Jaskulski

Agenda

1. State of the Internet
2. Why use protection?
3. Choose wisely – you get what you pay for

The numbers of Akamai

The Akamai Intelligent Platform

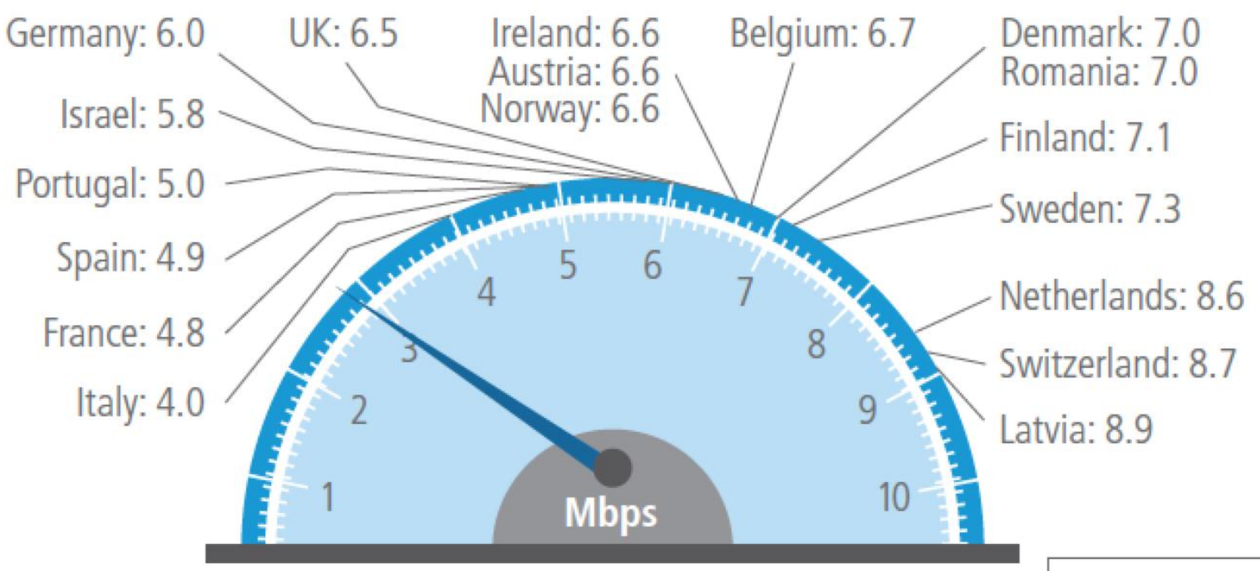
130,000+	1,100+	2,000+	700+	80
Servers	Networks	Locations	Cities	Countries

- Average traffic levels of over 6 Tbps
- Peak traffic levels to date of ~10Tbps
- Handling ~20 million hits/second, on average

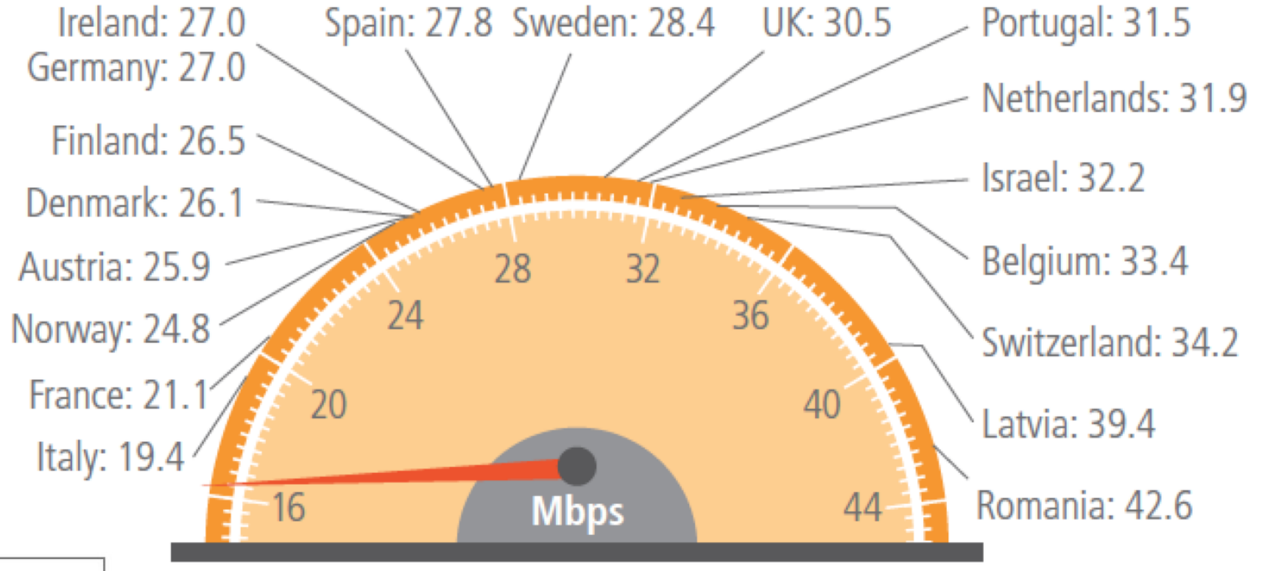
Close to the edge of the internet

90% of Internet users are within one network hop of an Akamai server

State of the internet



Average Connection Speeds, EMEA



Average Peak Connection Speeds, EMEA

2.9 Mbps
Global Average Connection Speed

16.6 Mbps
Global Average Peak Connection Speed

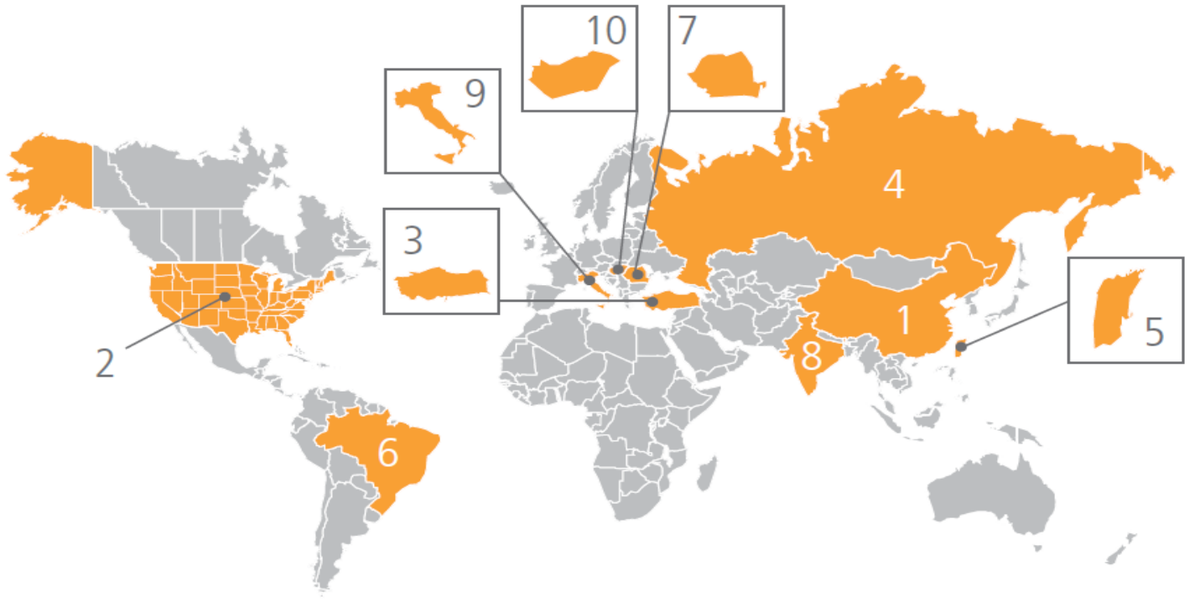
- 5% average connection speed increase
- 4.6% average peak speed increase

- 2.4% increase in unique IP v4 addresses

Where do attacks come from?

- Attacks coming from wide range of countries (117 unique countries in Q4 2012)
- Rise in attacks originating from China – now account for 41% of worldwide attack traffic
- Akamai's customers reported 758 DDoS attacks in 2012 (more than 3 times the amount seen in 2011)

	Country	Q4 '12 % Traffic	Q3 '12 %
1	China	41%	33%
2	United States	10%	13%
3	Turkey	4.7%	4.3%
4	Russia	4.3%	4.7%
5	Taiwan, Province of China	3.7%	4.5%
6	Brazil	3.3%	3.8%
7	Romania	2.8%	2.7%
8	India	2.3%	2.5%
9	Italy	1.6%	1.7%
10	Hungary	1.4%	1.4%
–	Other	25%	28%

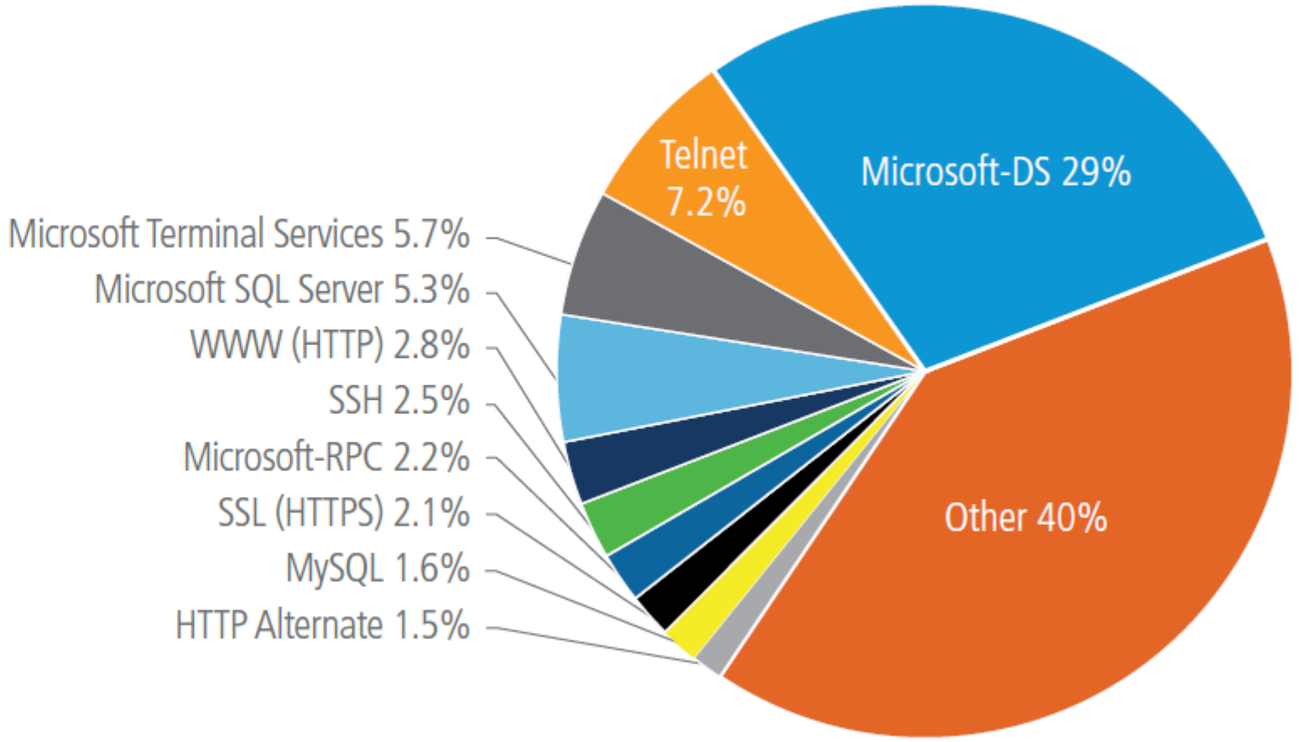


Attack trends

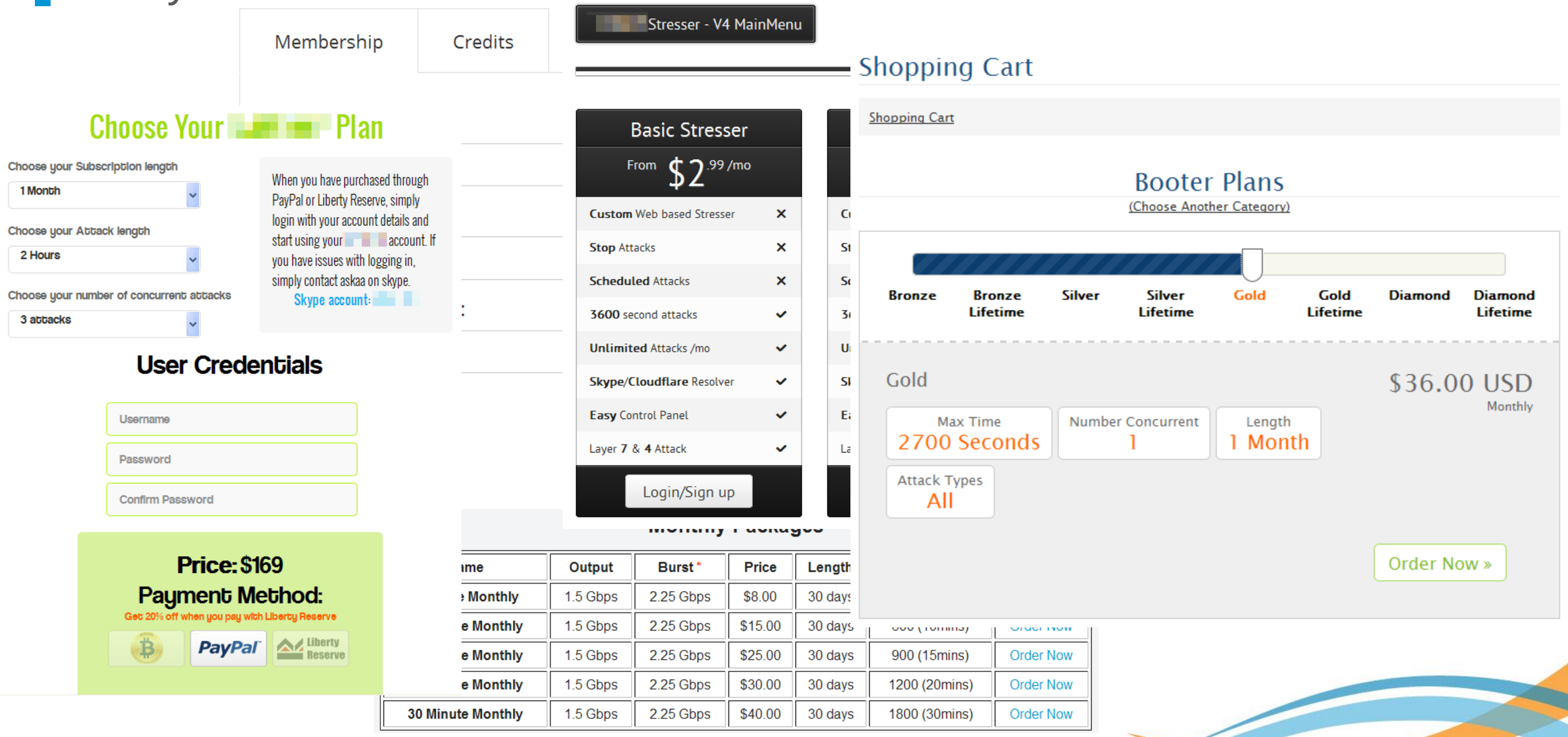
- Average attack bandwidth up 718 percent from 5.9 Gbps to 48.25 Gbps
- Average attack duration increased by 7.14 percent from 32.2 hours to 34.5 hours
- Regional distribution:
  - 56% Asia
  - 25% Europe
  - 18% North & South America
  - 1% Africa

What's your favorite port?

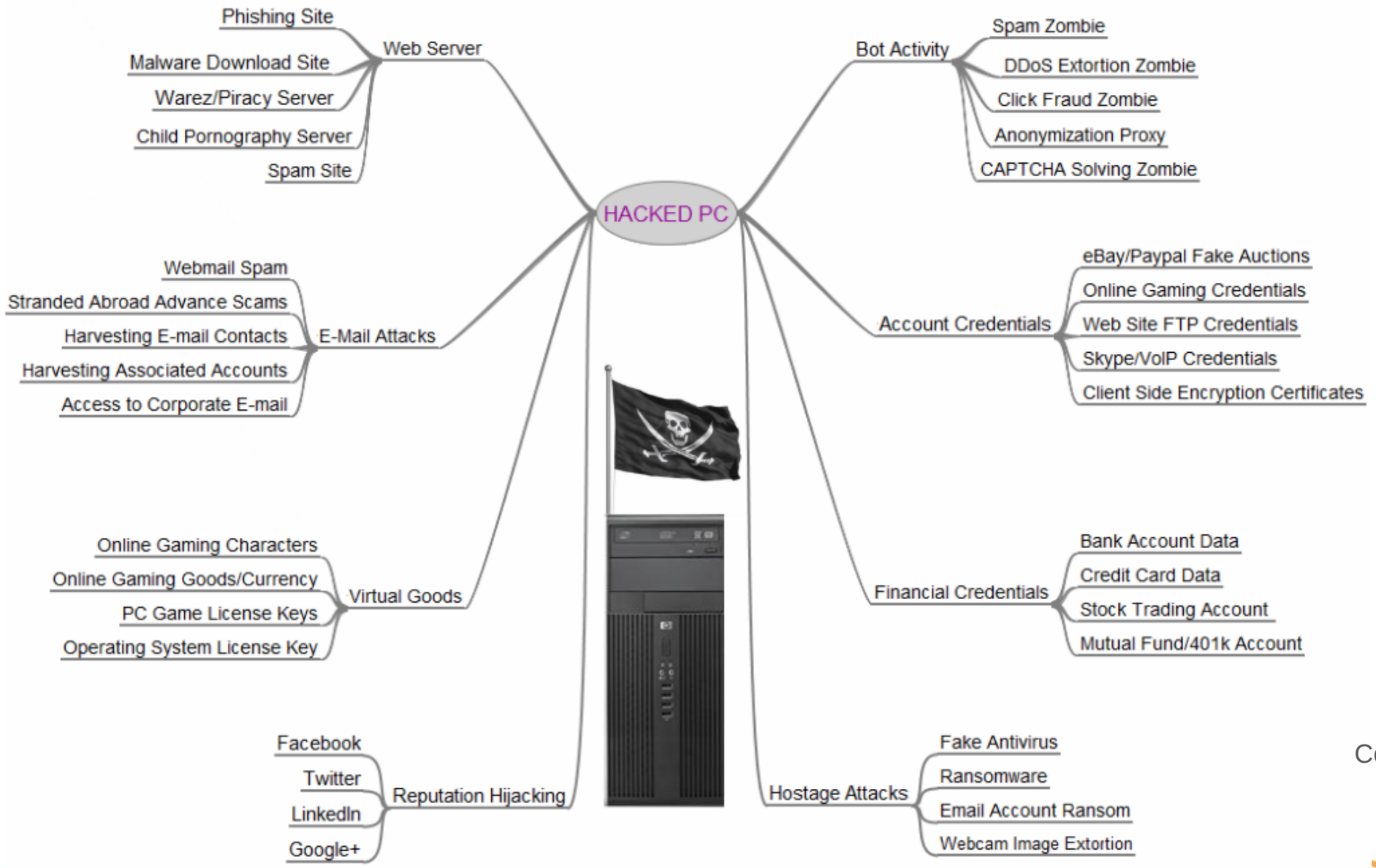
Port	Port Use	Q4 '12 % Traffic	Q3 '12 %
445	Microsoft-DS	29%	30%
23	Telnet	7.2%	7.6%
3389	Microsoft Terminal Services	5.7%	4.9%
1433	Microsoft SQL Server	5.3%	4.9%
80	WWW (HTTP)	2.8%	3.0%
22	SSH	2.5%	2.3%
135	Microsoft-RPC	2.2%	2.0%
443	SSL (HTTPS)	2.1%	1.1%
3306	MySQL	1.6%	1.3%
8080	HTTP Alternate	1.5%	1.7%
Various	Other	40%	–



Fancy an attack?



Value of a hacked machine



Courtesy of http://krebsonsecurity.com/

Real life example

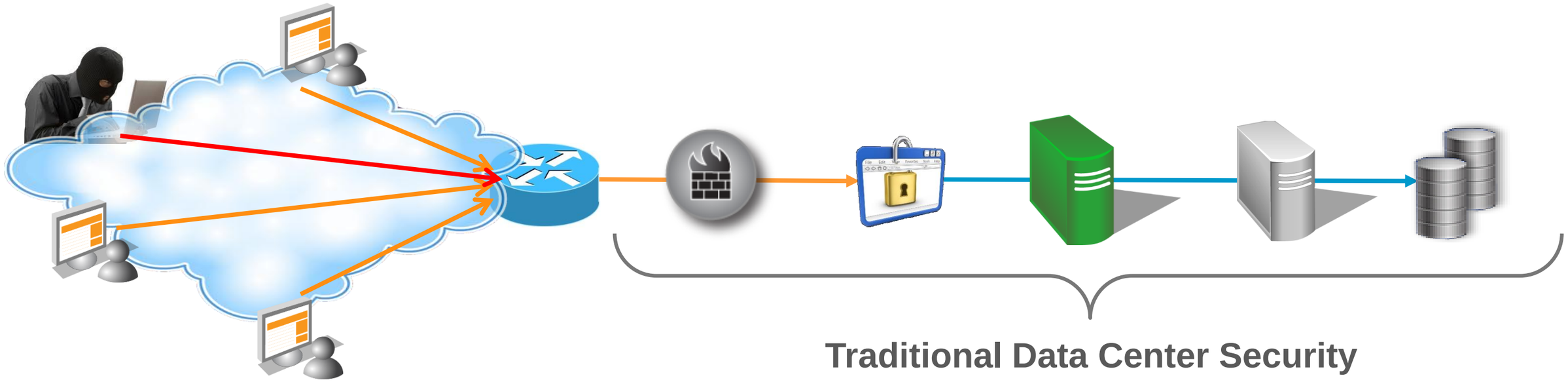
- **Top 500** online retailer generating just under **100,000 USD per hour** in revenue
- Internationally coordinated DDoS attack
- Shifting attack sources
- Changing attack signatures
- Peak attack traffic at **~112 Gbps** (over 10000 more than usually)
- Akamai absorbed the attack traffic
- Savings of **~10 million USD** over a period of several days

What are my security choices?

- Inhouse solutions
- Dedicated security services

    1. Reactive (Scrubbers) – monitor the traffic on your own. In case of attack direct incoming traffic to go through a ‘scrubbing centre’.
    2. Proactive – always-on model, 24h protection, adjust only for new attack vectors

In house security



Traditional Data Center Security

Limited scalability

Self-managed or MSSP

Off the shelf solution

Scrubbers

Akamai

PROLEXIC
DDoS Attacks End Here.

radware

NEXUSGUARD™
E-Business uptime, delivered.

GIGENET™
DDoS Protection since 1999

Incapsula

Black Lotus
communications

RACK911

ARBOR
NETWORKS

BLOCKDOS
DOS
Your Business, Our Protection

VERISIGN™

Akamai

- Distributed Intelligent Platform
- Security and Acceleration capabilities
- Several attack types dropped by default
- „Always on” protection
- Full control over features and configuration
- Real-time monitoring
- Acceleration, caching and more

Akamai Intelligent Platform basic protection levels

- TCP SYN flood attacks
- UDP flood
- ICMP flood
- Some HTTP response splitting attacks (when the split is in the URL path)
- Malformed request
- Port scanning
- Some basic DDoS protection (due to caching)

Akamai Security Portfolio

Enhanced DNS:
Attack against the DNS infrastructure
Attack against the TLD (customer.com)
BIND vulnerability exploits
Basic DNS poisoning attacks (TSIG)
Advanced DNS poisoning attacks (DNSSEC)

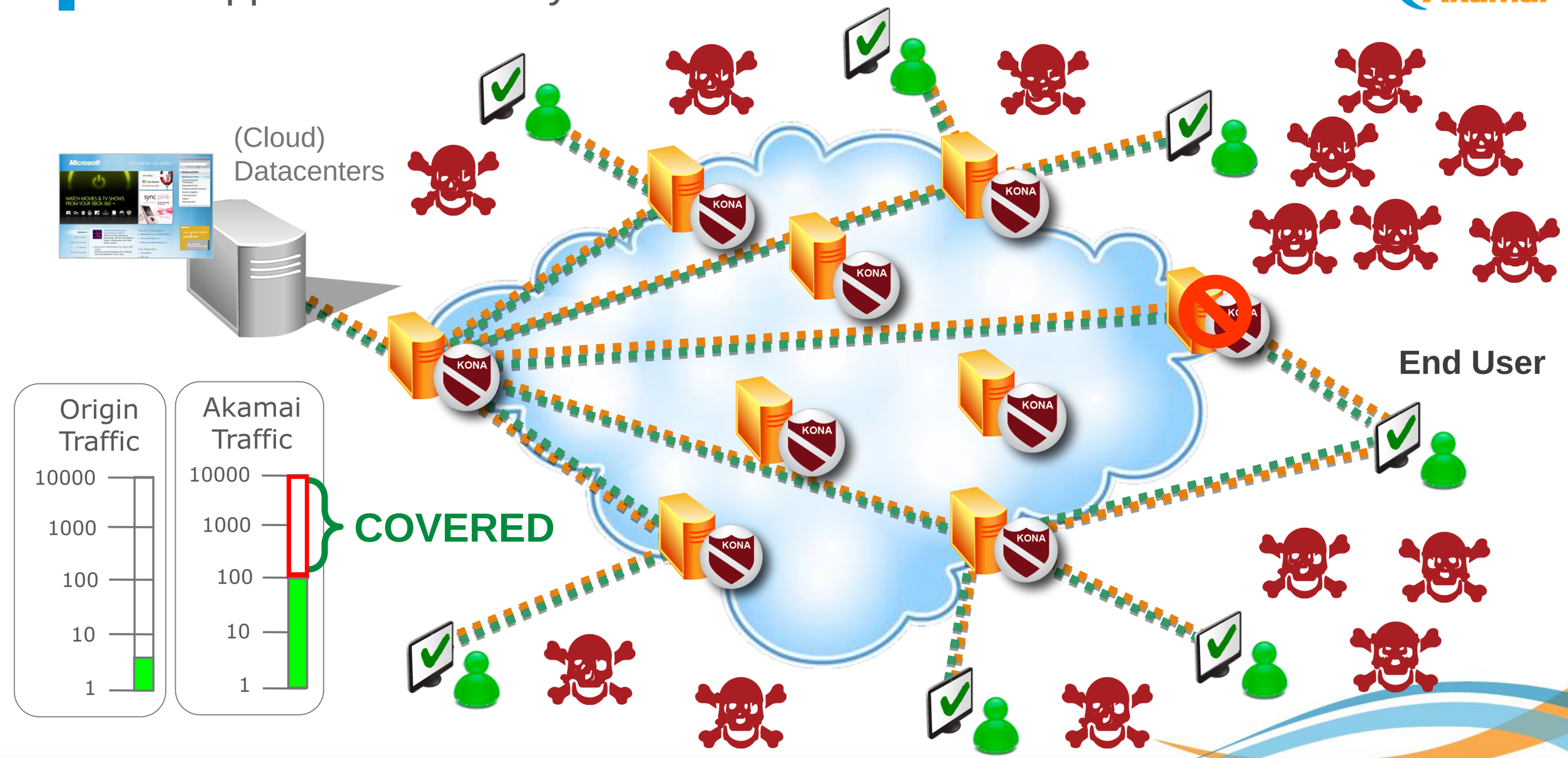
Web Application Firewall:
IP/CIDR/Geo whitelisting/blacklisting
XSS, SQLi
Protocol violations, Encoding abuse
Layer 7 floods

SiteShield:
Any layer 4-7 attacks directly against the origin
Still a risk to over at the layer 3

GTM:
Data center failure (load balancing, failover)

Shopper Prioritization:
Flash crowd (real or DDoS)

Web Application security with Akamai



Comparison

	In-house	Scrubbers	Akamai
Pricing model	Whatever you are willing to pay	Moderate Monthly Fee + Processed Traffic	Monthly Fee + Traffic (Insurance option)
Protection	Depending on what is installed	On request	Always on
Monitoring	Internal	Limited - customer mostly	Monitoring cockpits, InfoSec team notifications on ongoing and planned attacks
Integration	None (Internal)	For each attack: BGP route modification, GRE tunnel configuration	Once: DNS entry modification
Ports	-	All	80 & 443
Performance	Possible decrease	Decrease when activated	Increase due to accelerated

DDoS cheat sheet

- Decision makers list
- Define escalation paths
- Who to call and when (emergency contact information)

Check out our app

iTunes Preview

Akamai Internet Visualization App

By Akamai

Open iTunes to buy and download apps.

View In iTunes

This app is designed for both iPhone and iPad

Description

What does Internet traffic actually look like? Is it
How does the world's largest distributed comput

Akamai Web Site ▸ Akamai Internet Visualiz
Agreement ▸

What's New in Version 1.2

updated NetSessions feed

Questions?

Under attack? Call us!

www.ddos-hotline.com

Thank you!

Visit our booth at