Akamai

FASTER FORWARD

2nd SIG-NOC meeting and DDoS Mitigation Workshop
Scrubbing Away DDOS Attacks

9th November 2015

AKAMAI SOLUTIONS

WEB PERFORMANCE SOLUTIONS	MEDIA DELIVERY SOLUTIONS	CLOUD SECURITY SOLUTIONS	CLOUD NETWORKING SOLUTIONS	NETWORK OPERATOR SOLUTIONS
Accelerate websites to grow revenue and conduct business globally – on any device, anywhere	Deliver the ultimate in quality at scale, at reasonable cost	Secure websites and data centers to reduce the risk of downtime and data theft	Transform the enterprise network to accelerate applications, lower costs, and connect to clouds	Optimize network traffic, enable new revenue streams and control costs

SERVICES & SUPPORT

Akamai

Experience

17 years Experience in protecting against **DDoS** and **Web attacks**

Infrastructure

15 to **30** percent of global Web traffic

26 Tbps record traffic on our platform

Defending against **10** to **15** DDoS attacks every day

2,300 Gbps of dedicated attack capacity

Customers

1,350 Over 1350 customers

eCommerce

Media

And more…

2014

100 **Banks** worldwide use Akamai security solutions

Protecting the largest online events, including the **2014 Sochi Olympics** and **SuperBowl XLVIII**

Proof

320 **Gbps** **71.5** **Mpps** Largest DDoS attack mitigated, Q3 2014

History of DDOS – 3 gen

1st Generation DDoS Bots

- Infection – Workstation
- Command Communication – Bots pulled instruction
- 10 – 30,000 nodes needed to generate large attack (40 Gbps)
- Attacks ramped slowly

2nd Generation DDoS Bots (Brobot) Jan 2012

- Infection – Servers
- Command Communication – PUSH to bots
- 1 - 3,000 nodes needed to generate large attack 190Gbps
- Attacks ramped FAST 50-100Gbps in less than 10 minutes

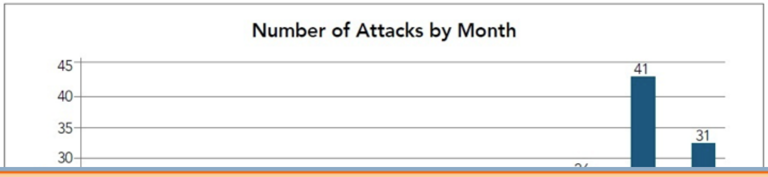
3rd Generation Reflection over Infection Blended Attacks

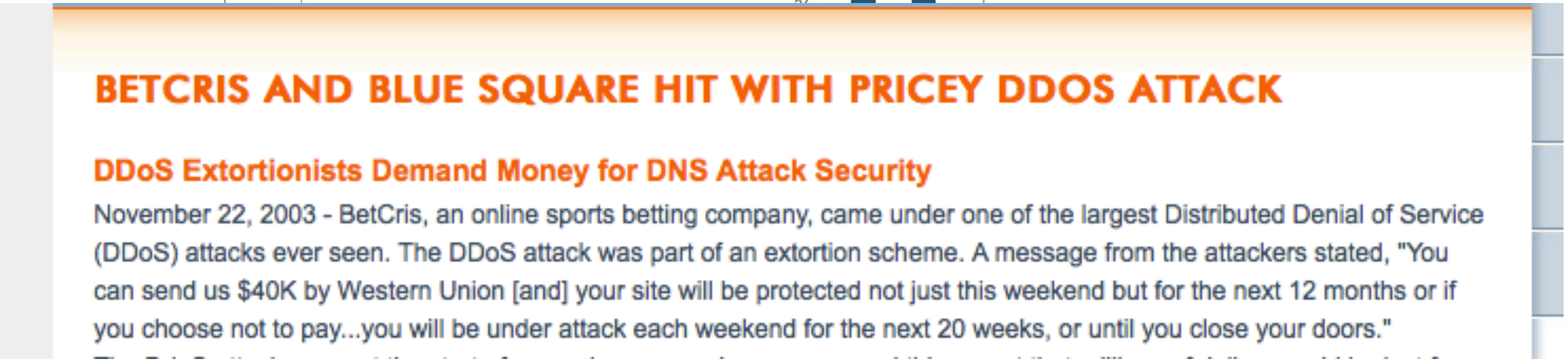
- Large Volumetric 320Gbps
- Abuse use of legitimate services
- Blended with DDoS attack tool kits for complexity (3 to 5 attack vectors)

Back to the bad old days

New actors – same script

- DD4BC





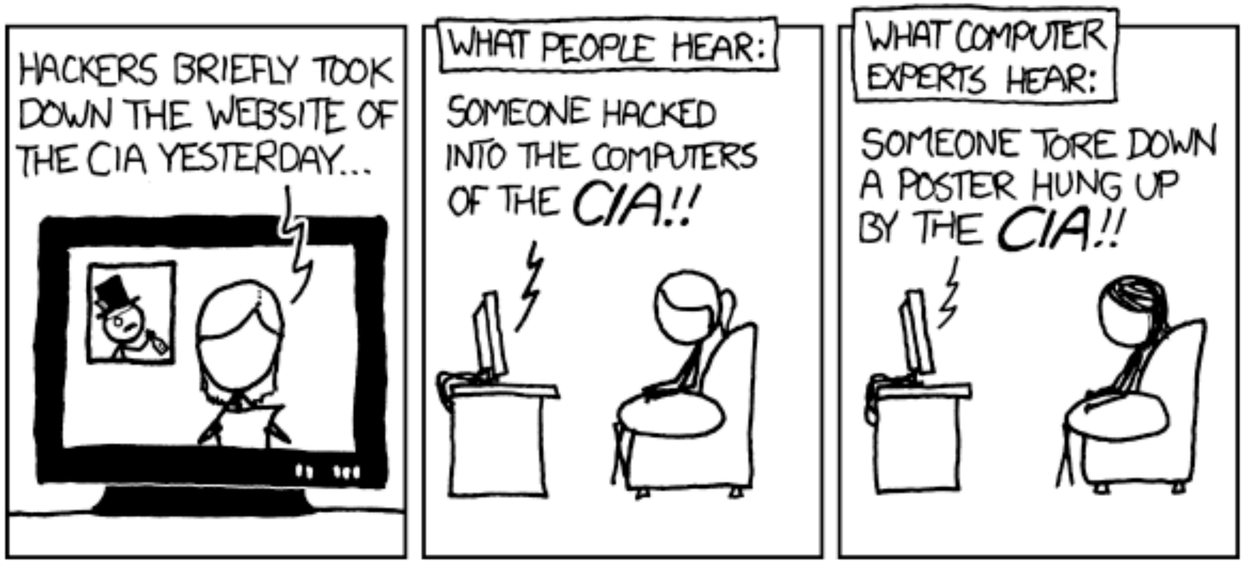
BETCRIS AND BLUE SQUARE HIT WITH PRICEY DDOS ATTACK

DDoS Extortionists Demand Money for DNS Attack Security

November 22, 2003 - BetCris, an online sports betting company, came under one of the largest Distributed Denial of Service (DDoS) attacks ever seen. The DDoS attack was part of an extortion scheme. A message from the attackers stated, "You can send us $40K by Western Union [and] your site will be protected not just this weekend but for the next 12 months or if you choose not to pay...you will be under attack each weekend for the next 20 weeks, or until you close your doors."

- A
  - Currently asking for 10-20 BC
  - Similar methodology to DD4BC – probably copycat rather than DD4BC renamed

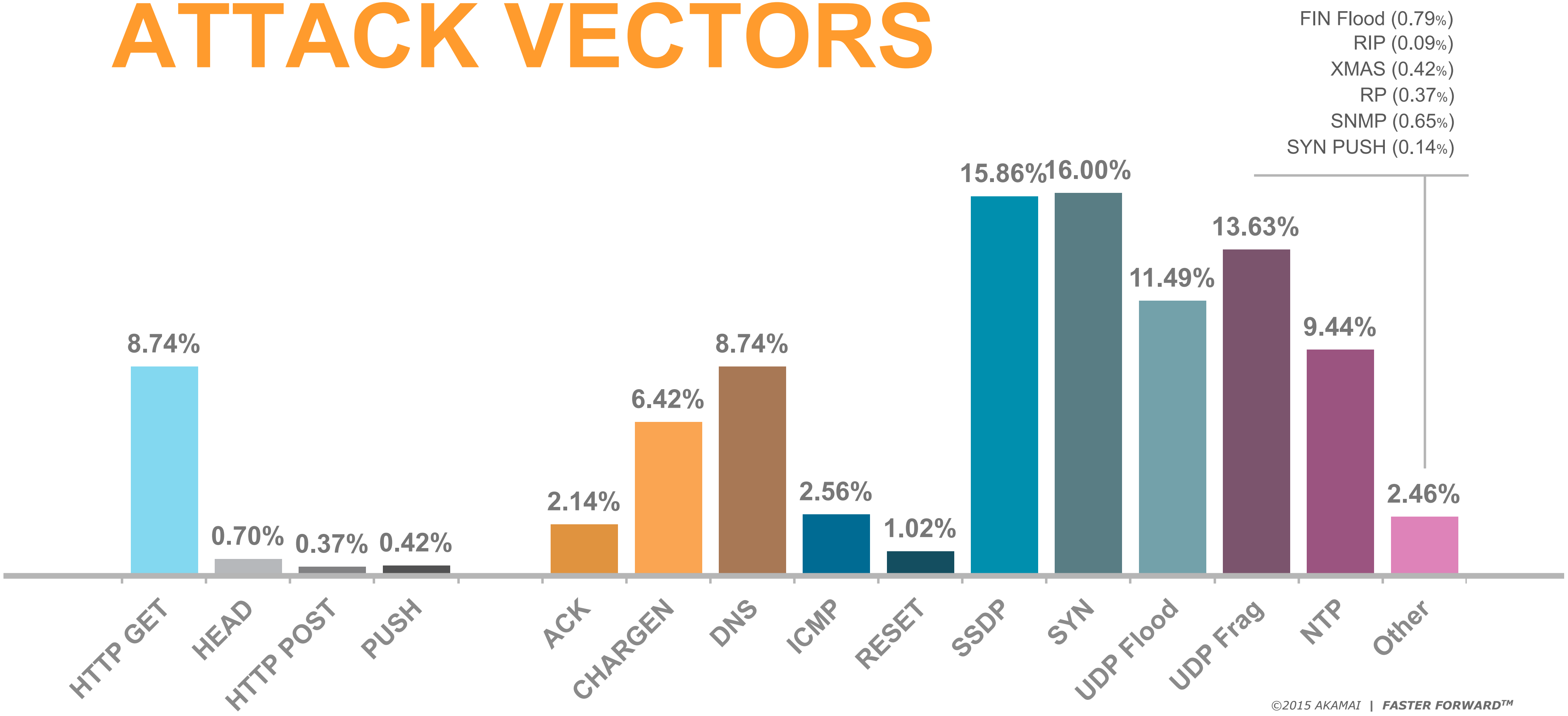
Public perception


HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

xkcd

Source: Akamai State of the Internet – Security, Q115

ATTACK VECTORS



New attacks

Threat Advisory released 28th October 2015

- Netbios Name Server
  - UDP port 137
  - Peak 15.7Gbps

- RPC Portmap
  - UDP port 111
  - Peak 105.96Gbps

- Sentinel Reflection DDOS
  - UDP 5093
  - 11.7Gbps

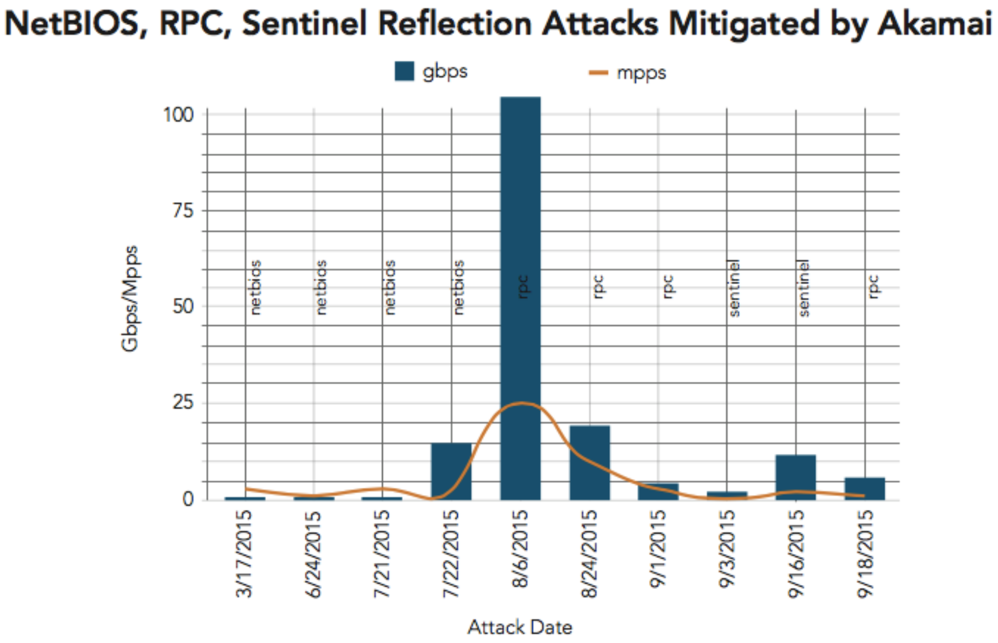
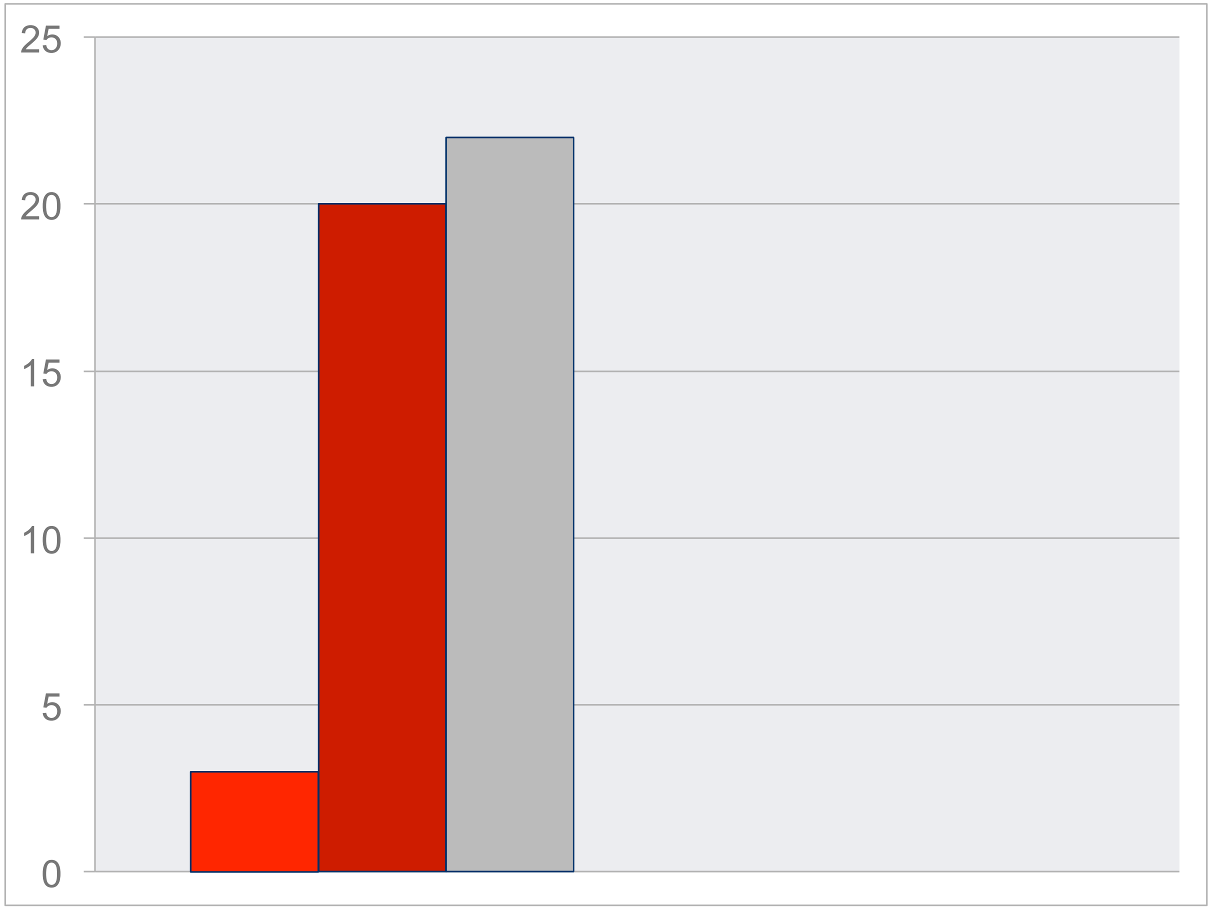


Figure 2: A timeline of NetBIOS, RPC portmap, and Sentinel reflection attacks. RPC portmap reflection generated the most traffic

How big is big?

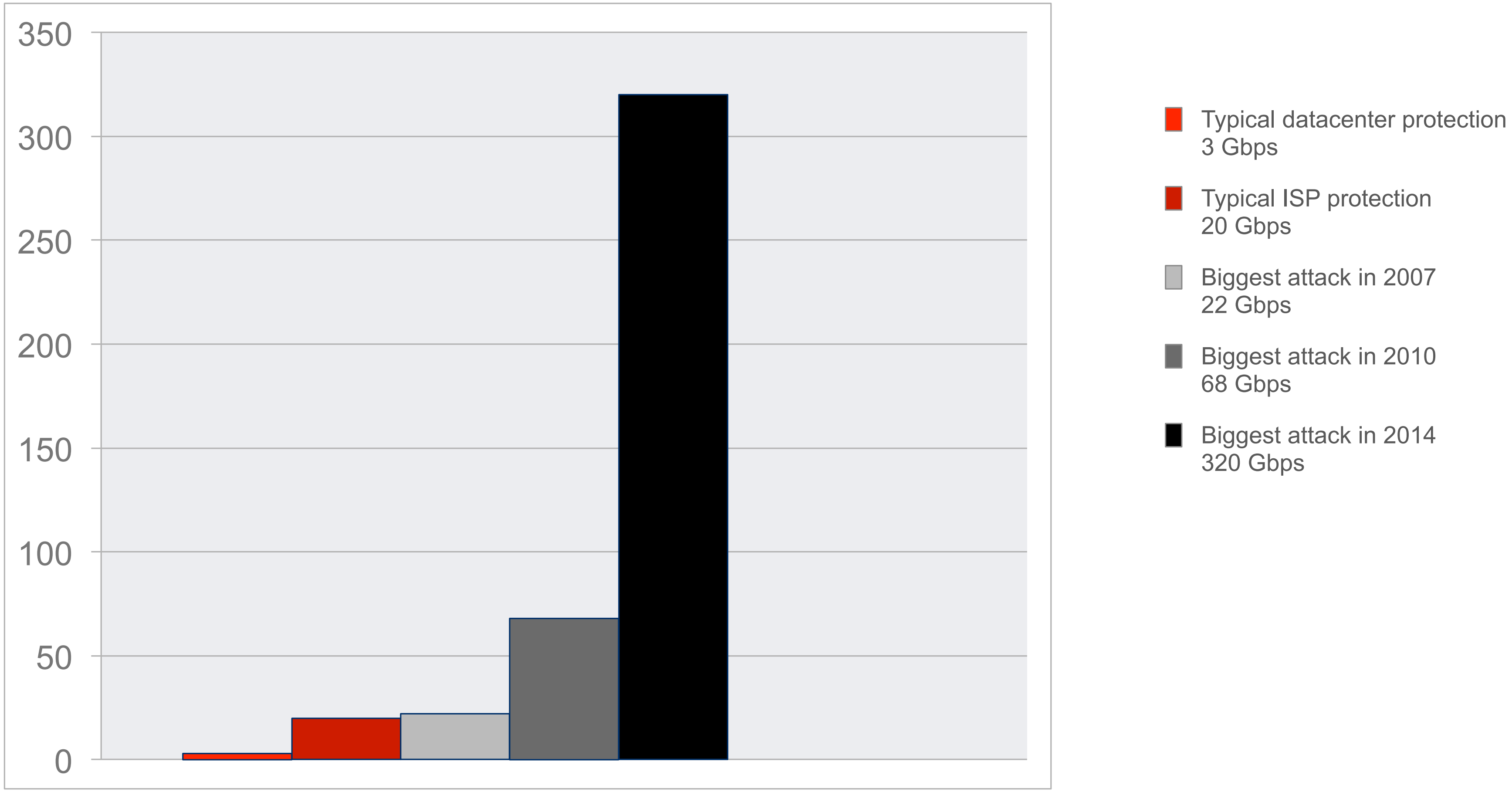


🟥 Typical datacenter protection
3 Gbps

🟥 Typical ISP protection
20 Gbps

⬜ Biggest attack in 2007
22 Gbps

How big is big?



🟥 Typical datacenter protection
3 Gbps

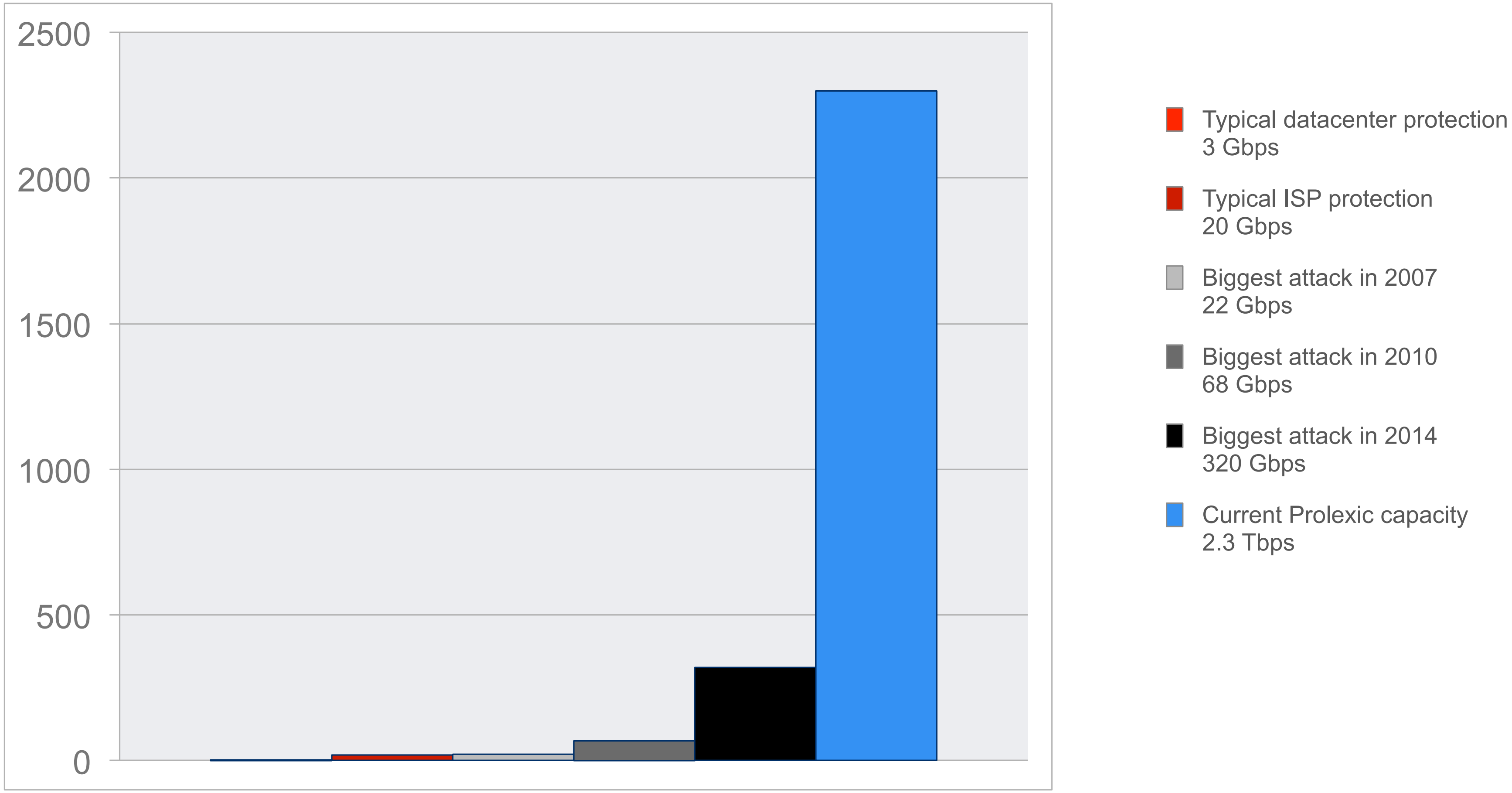
🟥 Typical ISP protection
20 Gbps

⬜ Biggest attack in 2007
22 Gbps

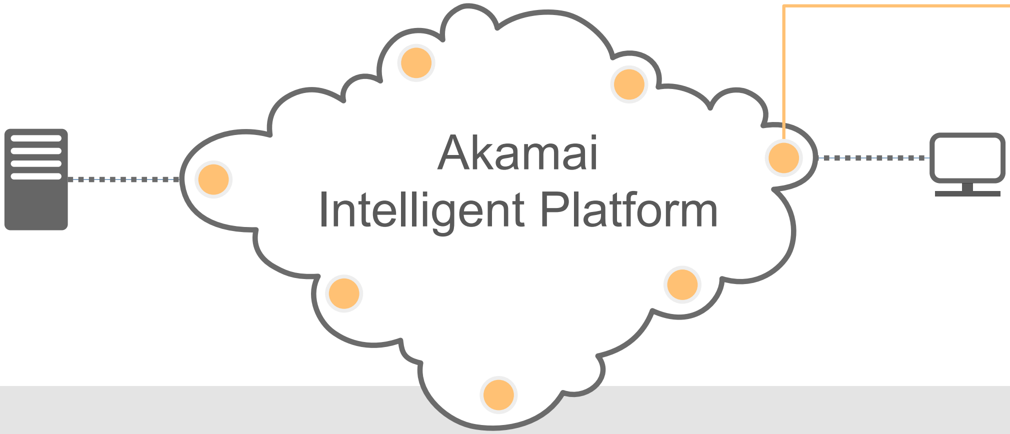
⬛ Biggest attack in 2010
68 Gbps

⬛ Biggest attack in 2014
320 Gbps

How big is big?



Globally distributed cloud platform

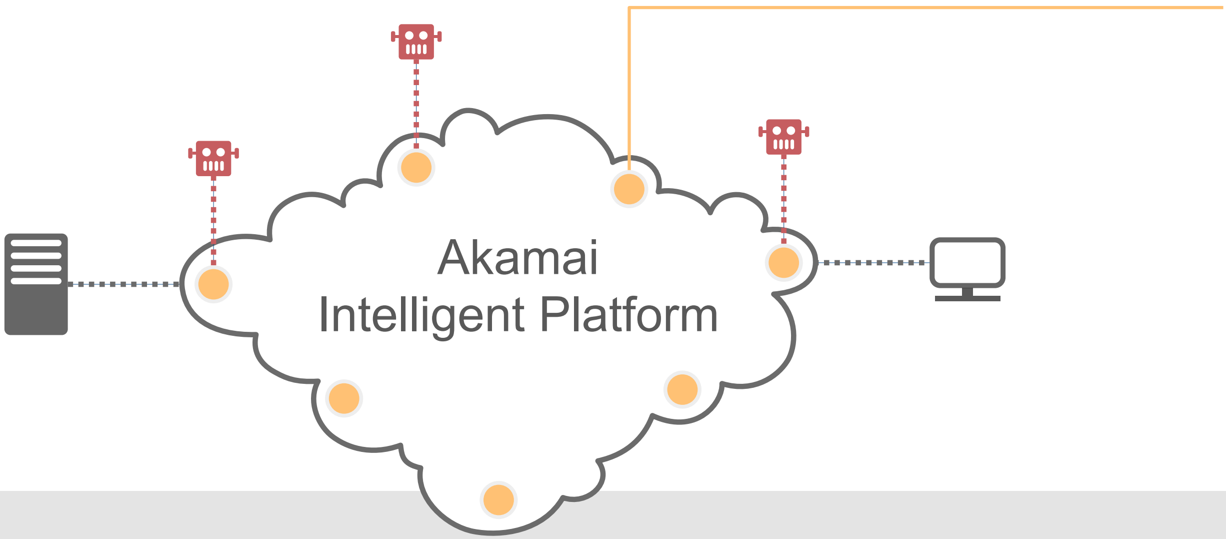


Scale | over 175,000 servers | seven scrubbing centers | more than 2,000 name servers

Distribution | 108 countries | over 2,700 locations | more than 1,300 networks

Resiliency | automatic failover within network | multiple networks for independent services

Integrated web security

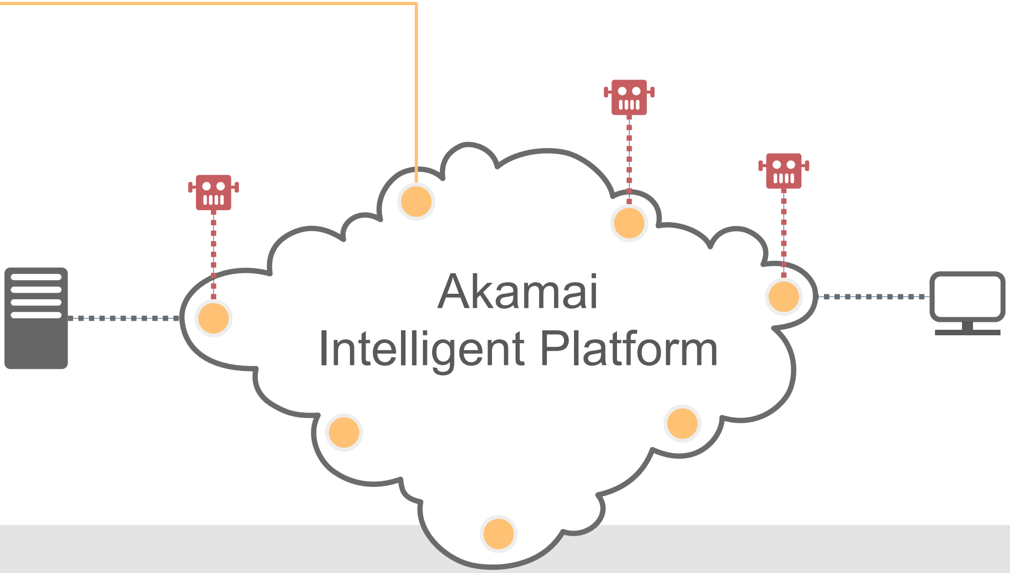


DDoS | always-on protection | automated response within seconds

WAF | proprietary rules engine | highly accurate | no performance impact

IP reputation | hundreds of millions of IPs monthly | customize policies based on risk of attack

Infrastructure protection

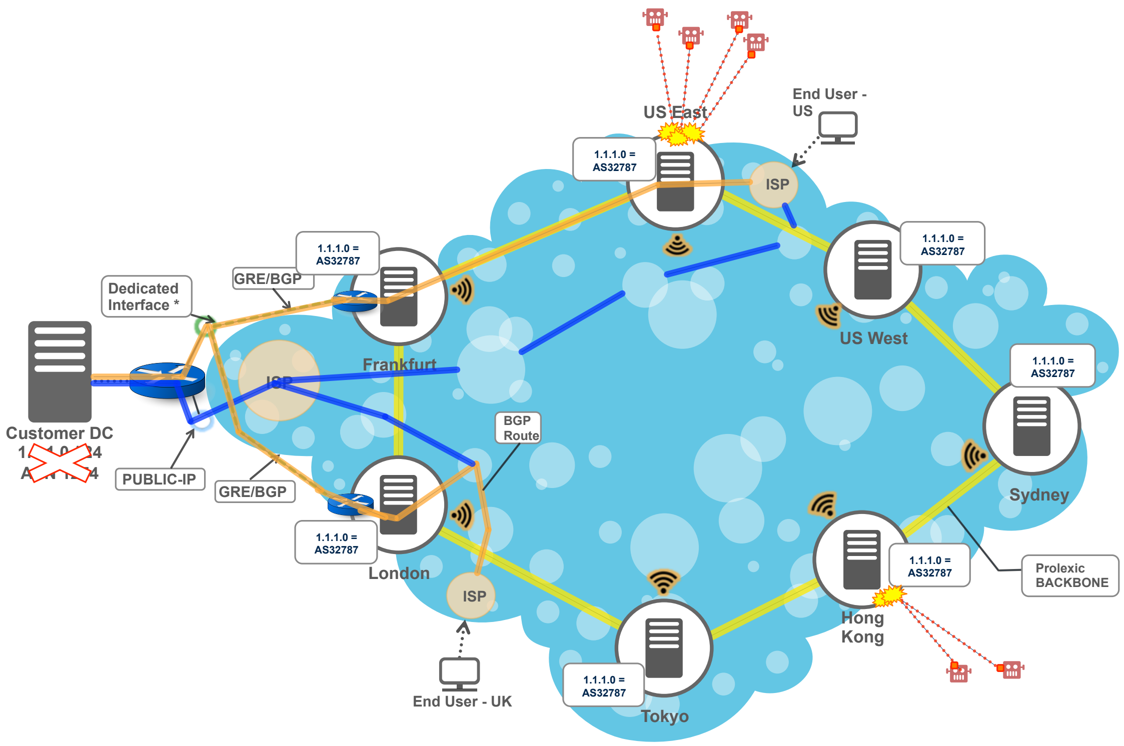


DDoS | people-driven response | customized mitigation | time-to-mitigate SLAs

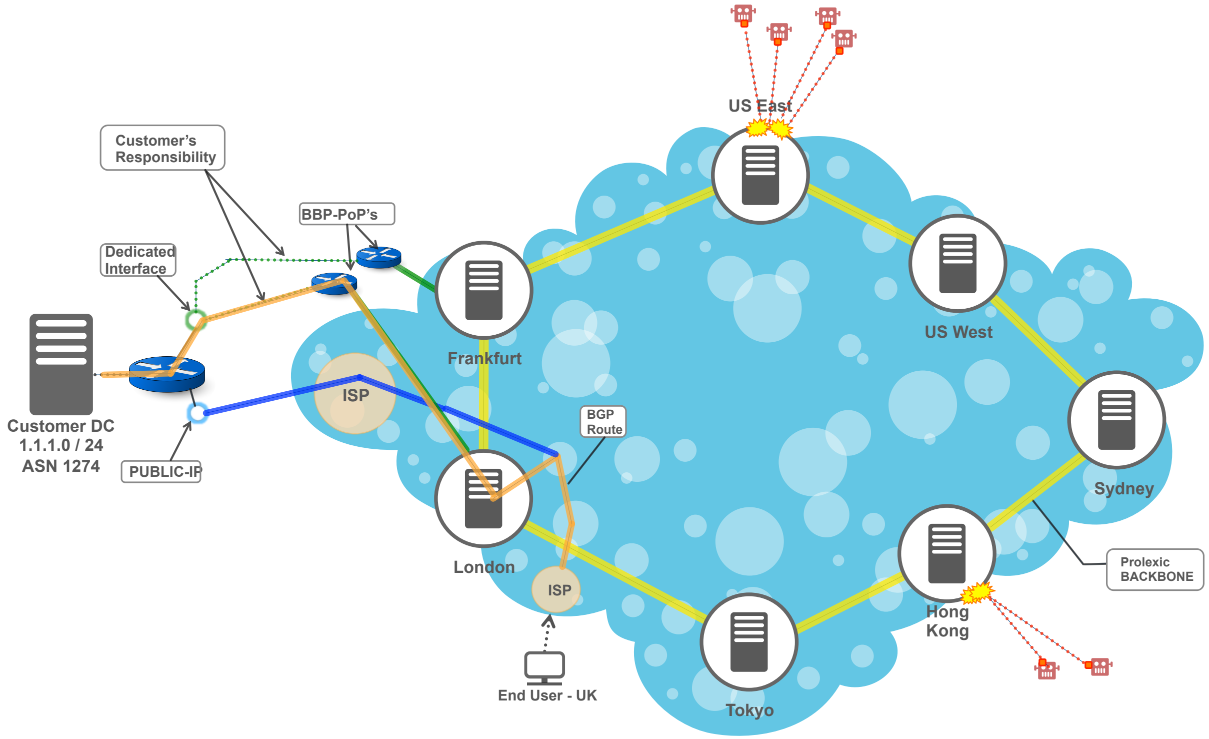
Data center | hundreds of applications | network infrastructure | Internet bandwidth

Flexible deployment | always-on or on-demand | 24x7 traffic monitoring

How does it work? – Prolexic (Routed)



How does it work? – Prolexic (Connect)



Commitment to

SECURITY EXPERTISE

Attack Type	**Time-to-Mitigate** (Typical)	**Time-to-Mitigate** (SLA)
UDP / ICMP floods	1 minute or less	5 minutes
SYN floods	1 minute or less	5 minutes
TCP flag abuses	1 minute or less	5 minutes
HTTP GET / POST floods	10 minute or less	20 minutes
DNS reflection	5 minute or less	10 minutes
DNS attack	5 minute or less	10 minutes

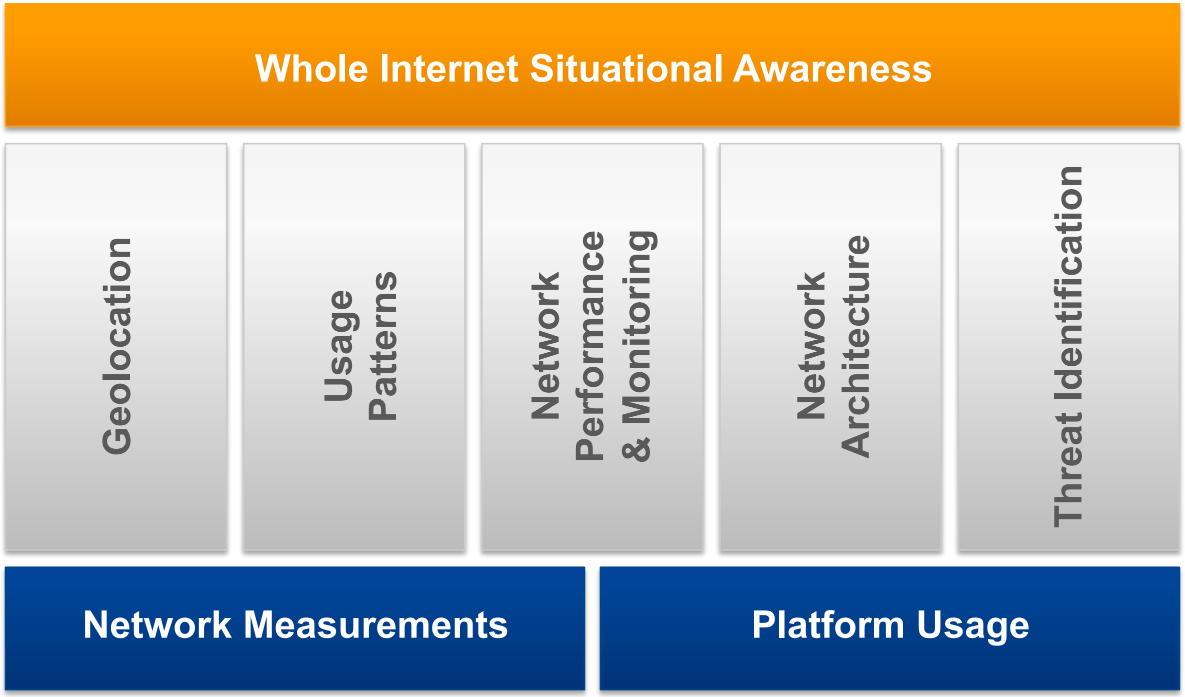
“Whole Internet Situational Awareness”

In a period of heightened awareness around “cyber terrorism”, Denial of Service attacks, and Internet disruptions,

“Whole Internet Situational Awareness”

is becoming increasingly important for both enterprises and governments

Whole Internet Situational Awareness through Akamai Data Feeds



Whole Internet Situational Awareness

Geolocation

Usage Patterns

Network Performance & Monitoring

Network Architecture

Threat Identification

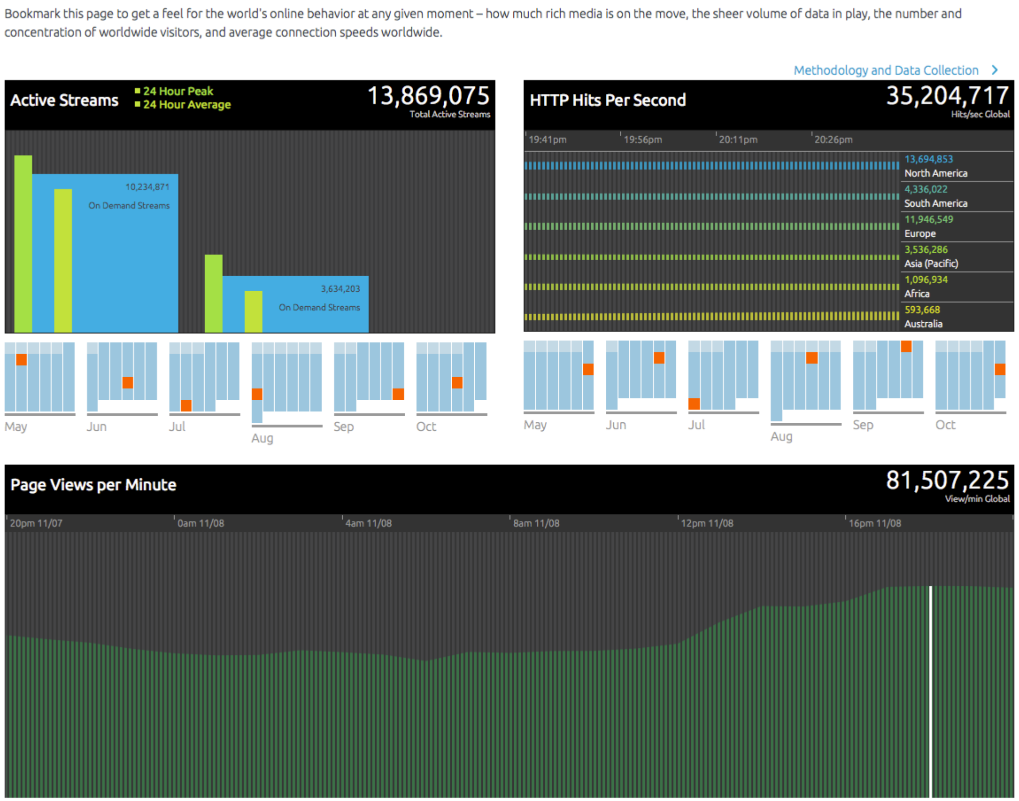
Network Measurements

Platform Usage

- Comprehensive and actionable insight
- Data is aggregated and analyzed
- Multiple categories of data feeds are produced
- Akamai both gathers and generates data

Data Feeds

- Global traffic views
  - Active streams
  - HTTP hits per second
  - Page views per minute



Bookmark this page to get a feel for the world's online behavior at any given moment – how much rich media is on the move, the sheer volume of data in play, the number and concentration of worldwide visitors, and average connection speeds worldwide.

Data Feeds

- Geolocation Database
- Usage Patterns
- Network Performance / Monitoring
  - Latency / Loss
  - State of the Internet
  - TCP stats
  - BGP Churn / Dump

- Network Architecture
  - Associated Client and Nameserver Addresses
  - Traceroutes
  - Client Nameserver
  - Network Correlation
  - Core Points
- Threat Identification
  - Darknet
  - Proxy Detection

Summary / Questions?

- Akamai supplies Industry leading cloud-based DDOS solutions
- Solutions tailoured for End-user and ISP / Hosting providers
- Leverages the 15-30% of global traffic seen everyday for the most current threats

Akamai

FASTER FORWARD