Advanced DDoS Defense

Gord Taylor, Global Practice Lead – Threat Protection Services

October 25, 2013

Agenda

- What is DDoS?
- Current State of DDoS Threats
- Do I need DDoS Mitigation Solution?
- DDoS Attack Types
- DDoS Mitigations
- Summary

Who am I?

- Gord Taylor (gtaylor@sentrymetrics.com)
- Sentry Metrics' Global Practice Lead – Threat Protection Services
- Advisor for SecTor Security Conference (www.sector.ca) since inception 7 Years ago
- 15 years in Information Security field
- 20 years working with Financial Institutions

SentryMetrics

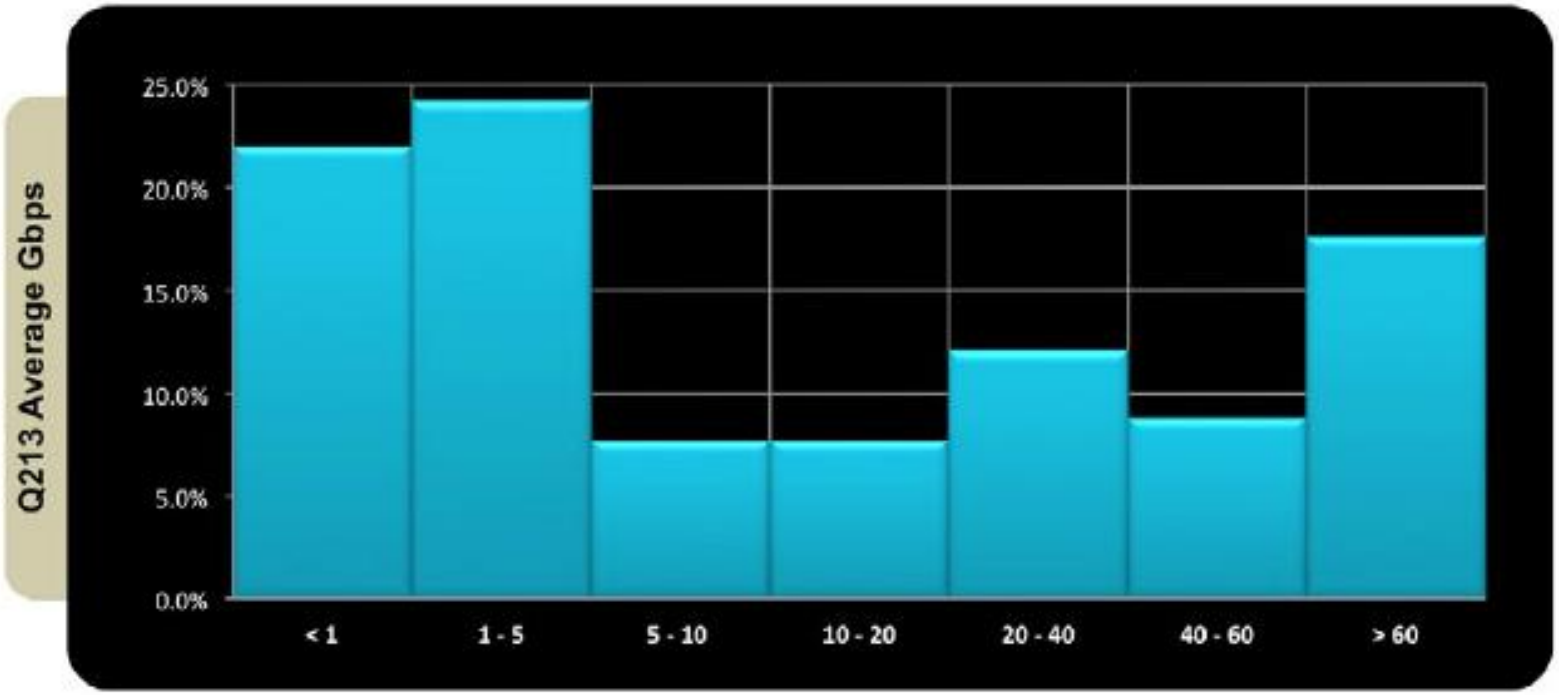
What is DDoS?

A Distributed Denial of Service (DDoS) attack is a deliberate attempt to make a computer system or network unavailable to its intended users.

Current State of DDoS Threats

- DDoS attacks are regularly exceeding 100Gbps rates
- Few companies can handle a sustained DDoS without assistance and/or dedicated tools
- Most ISPs will black hole your address space (route to Null0)
- DDoS attacks are on the rise
- DDoS is not going away, and most signs show it getting worse

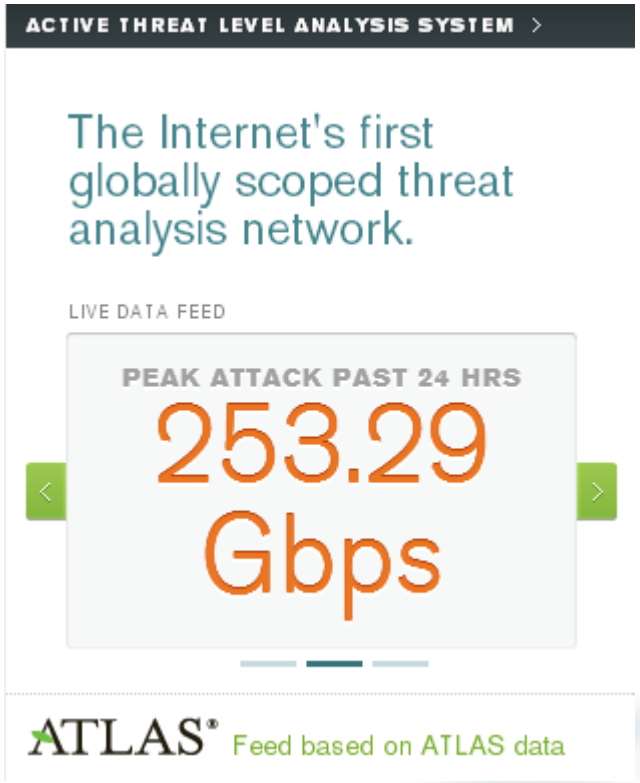
Current State of DDoS Threats

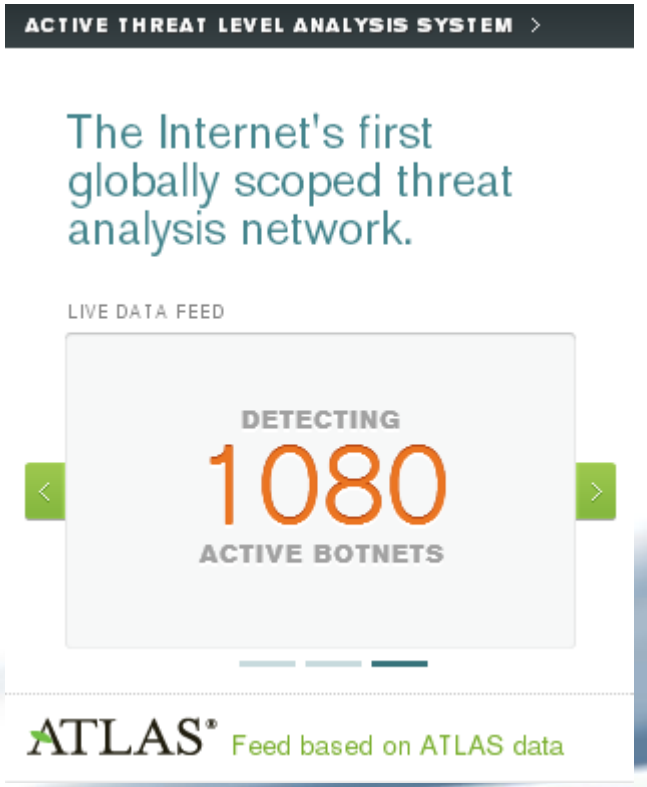


Prolexic Quarterly DDoS Attack Report Q2/2013

Current State of DDoS Threats

- Arbor Main Page (www.arbornetworks.com) – Oct 5, 2013





Do I need a DDoS Solution?

Targeted Customer Types

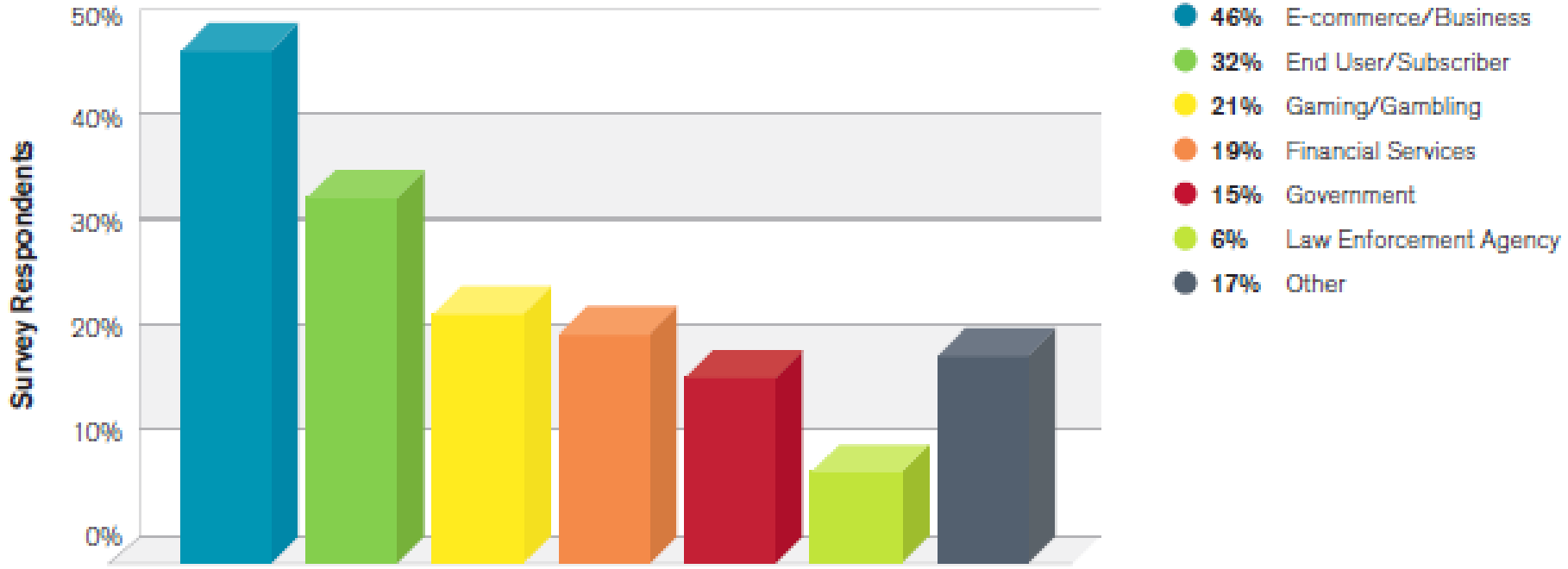


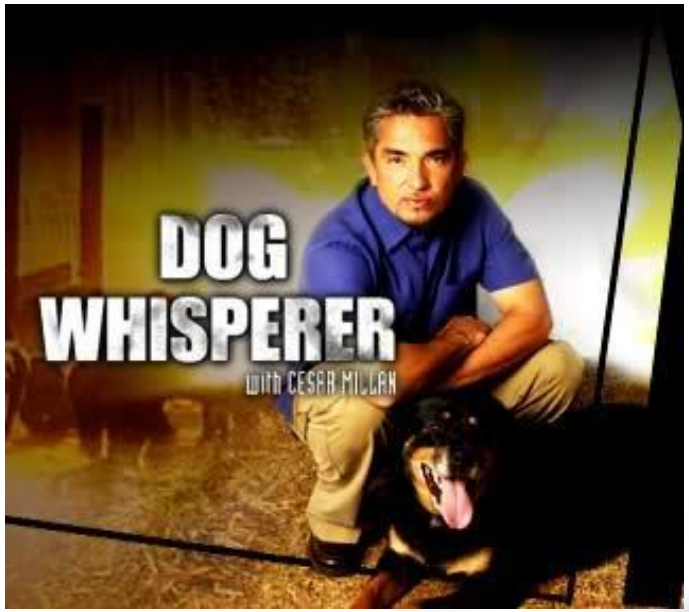
Figure 22 Source: Arbor Networks, Inc.

Arbor Worldwide Infrastructure SecurityReport 2012

He needed a DDoS Solution

- Anyone recognize this person?

- Cesar Millan – The Dog Whisperer

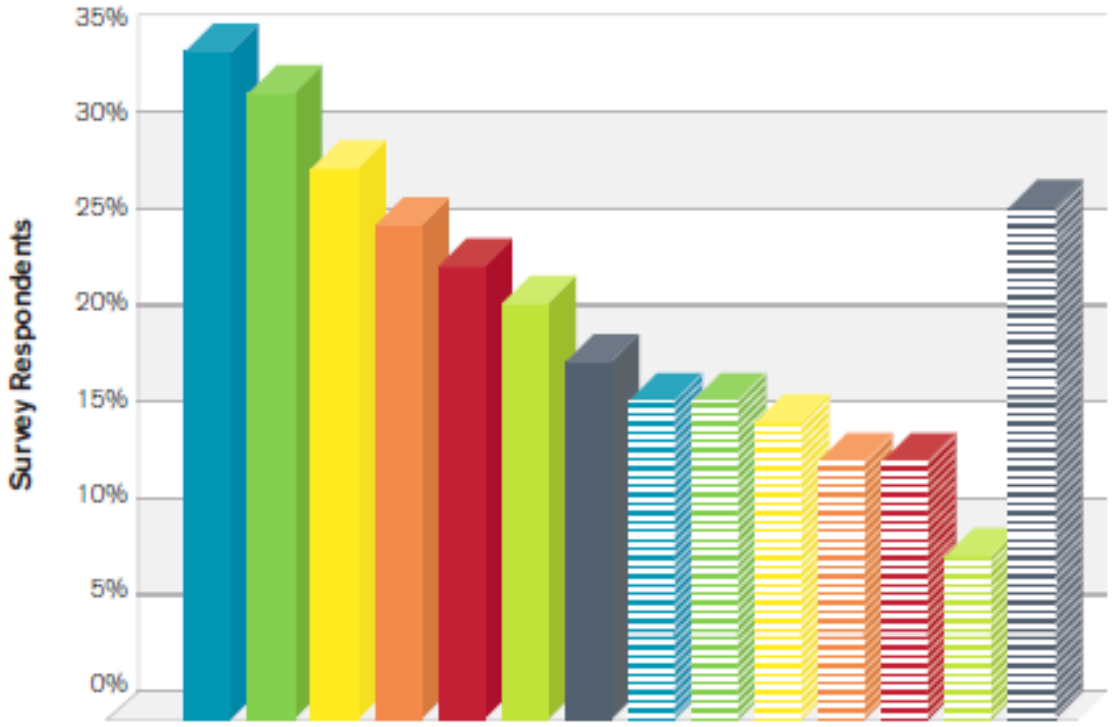


Motivation

- Political / Hacktivism
- Fun
- Extortion
- Distraction

Motivation

Most Common Motivations Behind DDoS Attacks



- **33%** Political/Ideological Disputes
- **31%** Online Gaming-Related
- **27%** Nihilism/Vandalism
- **24%** Criminals Demonstrating DDoS Attack Capabilities to Potential Customers
- **22%** Social Networking-Related
- **20%** Interpersonal/Inter-Group Rivalries
- **17%** Misconfiguration/Accidental
- **15%** Competitive Rivalry Between Business Organizations
- **15%** Diversion to Cover Compromise/Data Exfiltration
- **14%** Criminal Extortion Attempts
- **12%** Flash Crowds
- **12%** Financial Market Manipulation
- **7%** Intra-Criminal Disputes
- **25%** Unknown

Figure 16 Source: Arbor Networks, Inc.

Arbor Worldwide Infrastructure SecurityReport 2012

SentryMetrics

Why do DDoS Attacks Continue to Succeed?

- Traditional security mitigation methods are reactive
- Traditional security tools are in the datacentre, so mitigation can only occur after traversing “last mile”
- Stateless protocols are still prevalent
- BotNets remain easy to create and hard to take down
- NAT usage requires allowing multiple sessions from single host

DoS Attack Types

- Protocol – Flaws in network protocol
  - SYN Flood, Fragmented Packet Flood, Ping of Death, Smurf
- Volumetric – Attack the network
  - UDP Floods, ICMP floods, Spoofed packet floods
- Application
  - Slowloris, SSL Handshake
- Self-Inflicted

Protocol Attacks

- Least used
- Typically attacks the network, not the server
- Often fails because the attackers ISP prevents the outbound packet
- New technologies such as IPv6, DNSSec, etc may cause an increase in these types of attacks
- THC IPv6 Attack Toolkit

  (updated Oct 12, 2013)

Volumetric Attacks

- Most prevalent attack type
- Most often used with stateless protocol (UDP)
- Source address can be spoofed
- DNS Reflection Attack is most frequent
- Favorite attack of BotNet owners

End-User Bandwidth is Increasing

Global Rank	Country/Region	Q1 '13 Avg. Mbps	QoQ Change	YoY Change
9	United States	8.6	7.4%	27%
13	Canada	7.8	7.8%	21%
57	Mexico	3.3	9.2%	19%
63	Chile	3.0	2.7%	-11%
64	Colombia	2.8	1.5%	5.8%
72	Ecuador	2.3	2.8%	34%
73	Brazil	2.3	4.4%	7.4%
78	Costa Rica	2.1	5.7%	19%
82	Argentina	2.1	4.7%	-6.6%
85	Peru	2.0	5.7%	24%
99	Uruguay	1.7	4.0%	29%
117	Paraguay	1.2	6.3%	-3.6%
123	Venezuela	1.1	5.1%	19%
128	Bolivia	0.9	-0.7%	51%

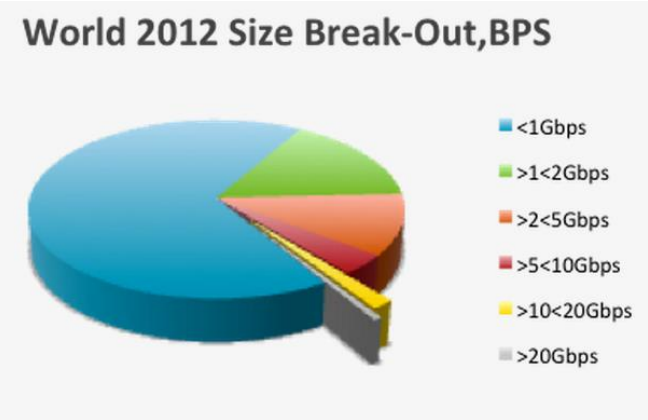
Figure 19: Average Connection Speed by Americas Country

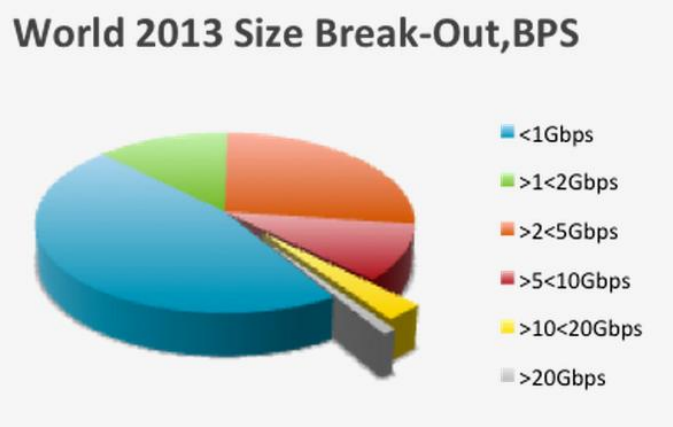
Global Rank	Country/Region	% Above 10 Mbps	QoQ Change	YoY Change
8	United States	25%	14%	69%
15	Canada	19%	22%	77%
45	Chile	0.9%	17%	-12%
46	Mexico	0.8%	41%	106%
47	Brazil	0.7%	13%	38%
48	Argentina	0.6%	28%	51%
–	Ecuador	0.7%	36%	179%
–	Costa Rica	0.6%	40%	56%
–	Colombia	0.2%	-20%	-44%
–	Peru	0.1%	1.7%	1.7%
–	Venezuela	0.1%	-1.9%	56%
–	Uruguay	0.1%	33%	767%
–	Bolivia	0.0%	-13%	100%
–	Paraguay	0.0%	-50%	-46%

Figure 21: High Broadband (>10 Mbps) Connectivity by Americas Country

Akamai State of the Internet Q1/2013

Key Findings: Attack sized increasing rapidly





- For 2013 an average DDoS attack now stands at 2.64Gb/sec, up 78% from 2012
- 54% of attacks so far this year are over 1Gb/sec, up from 33% in 2012
- 37% of attacks so far this year are in the 2 – 10 Gb/sec range, up from 15% last year
- 44% growth in proportion of attacks over 10Gb/sec, to 4% of all attacks
- More than 350% growth in the number of attacks monitored at over 20Gb/sec so far this year, as compared to the whole of 2012
- 87% of all attacks monitored so far this year last less than one hour
- Largest monitored and verified attack size increases significantly to 191Gb/sec

Arbor Networks Q3/2013 findings from Atlas (Oct 16, 2013)

Mobile – The New DDoS Attack Platform

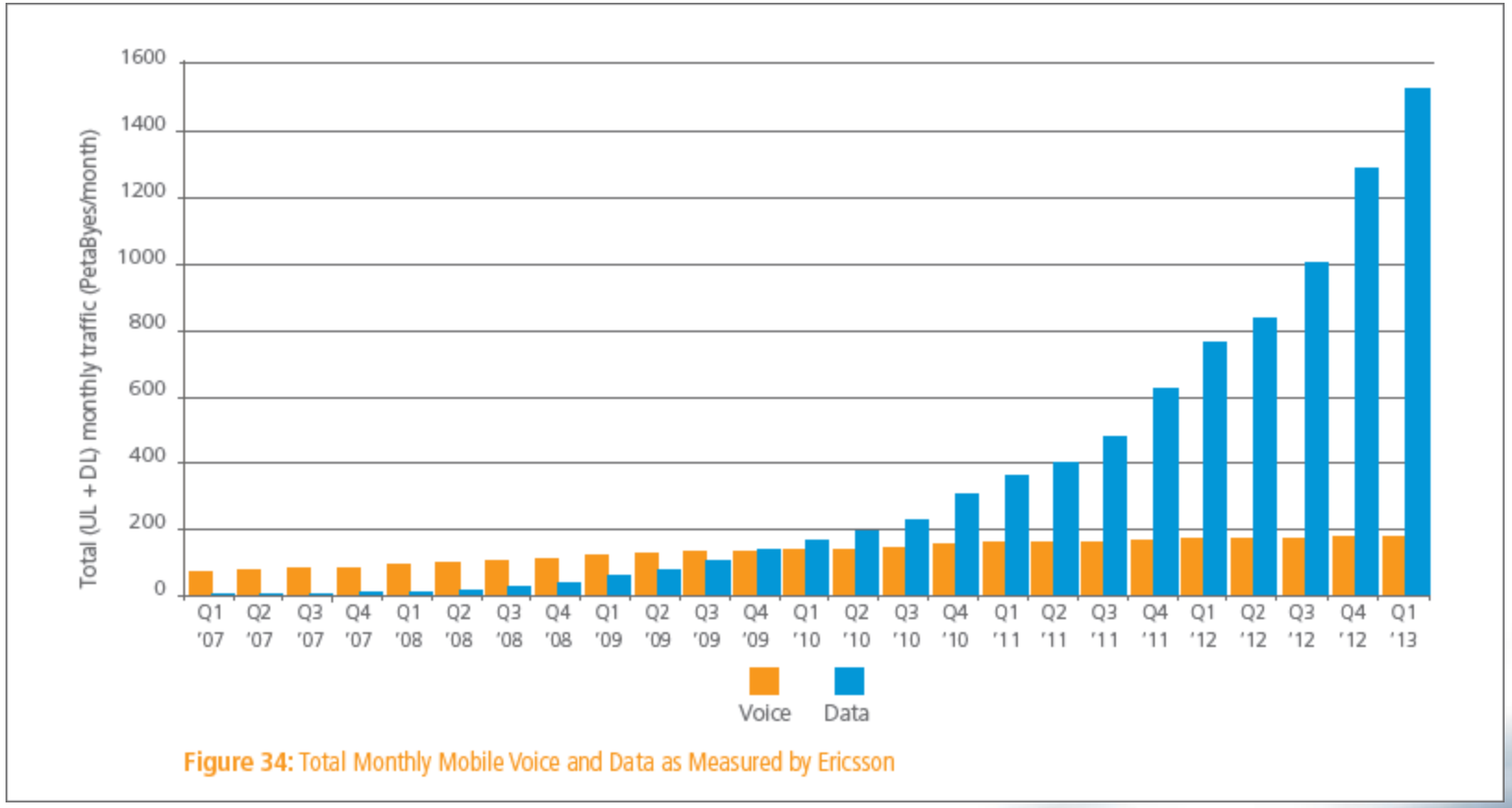


Figure 34: Total Monthly Mobile Voice and Data as Measured by Ericsson

Akamai State of the Internet Q1/2013

Application Attacks

- Typically TCP-based
- Typically require fewer clients than Volumetric attacks
- Target is typically to cause servers to consume excessive resources
- May attack business/application logic of web applications

What is Being Attacked

Targets of Application-Layer Attacks

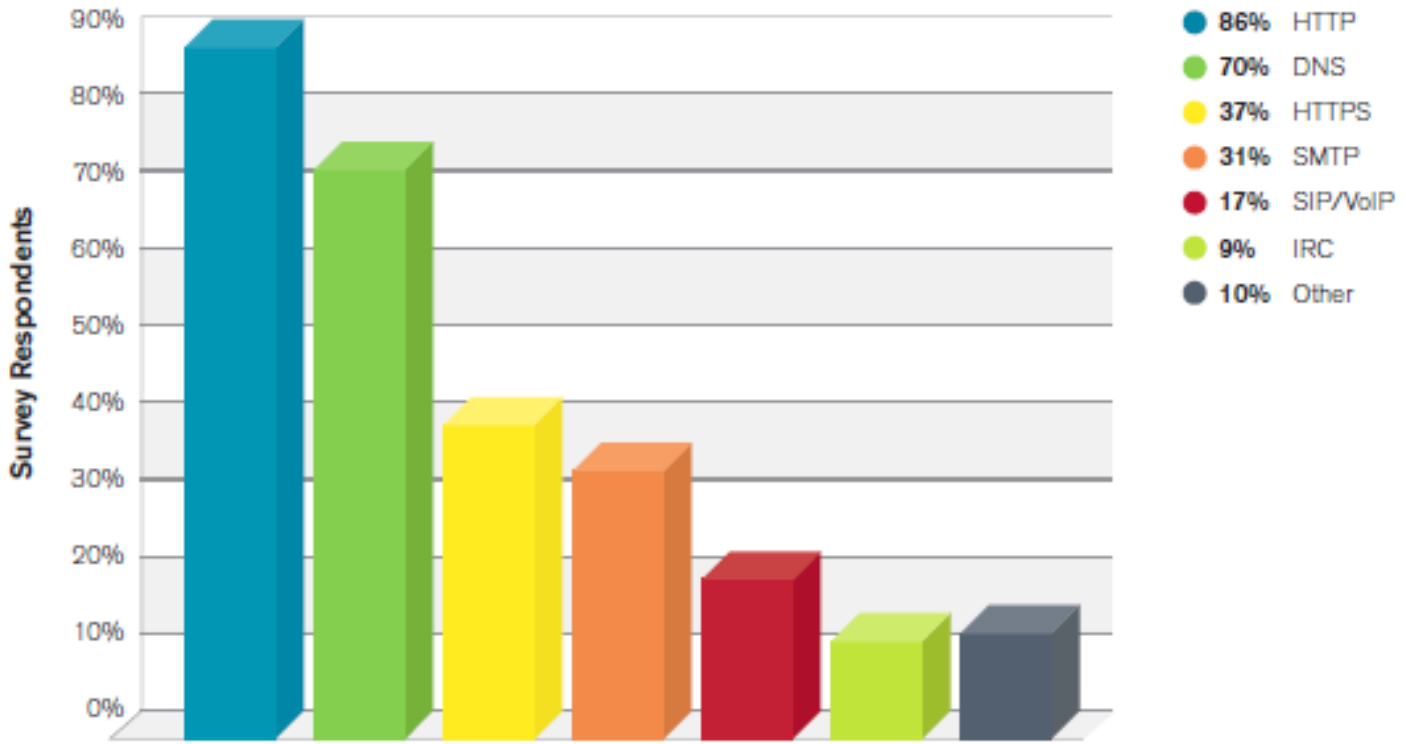


Figure 24 Source: Arbor Networks, Inc.

Arbor Worldwide Infrastructure SecurityReport 2012

How it is Being Attacked

Application-Layer Attack Vectors Targeting Web Services

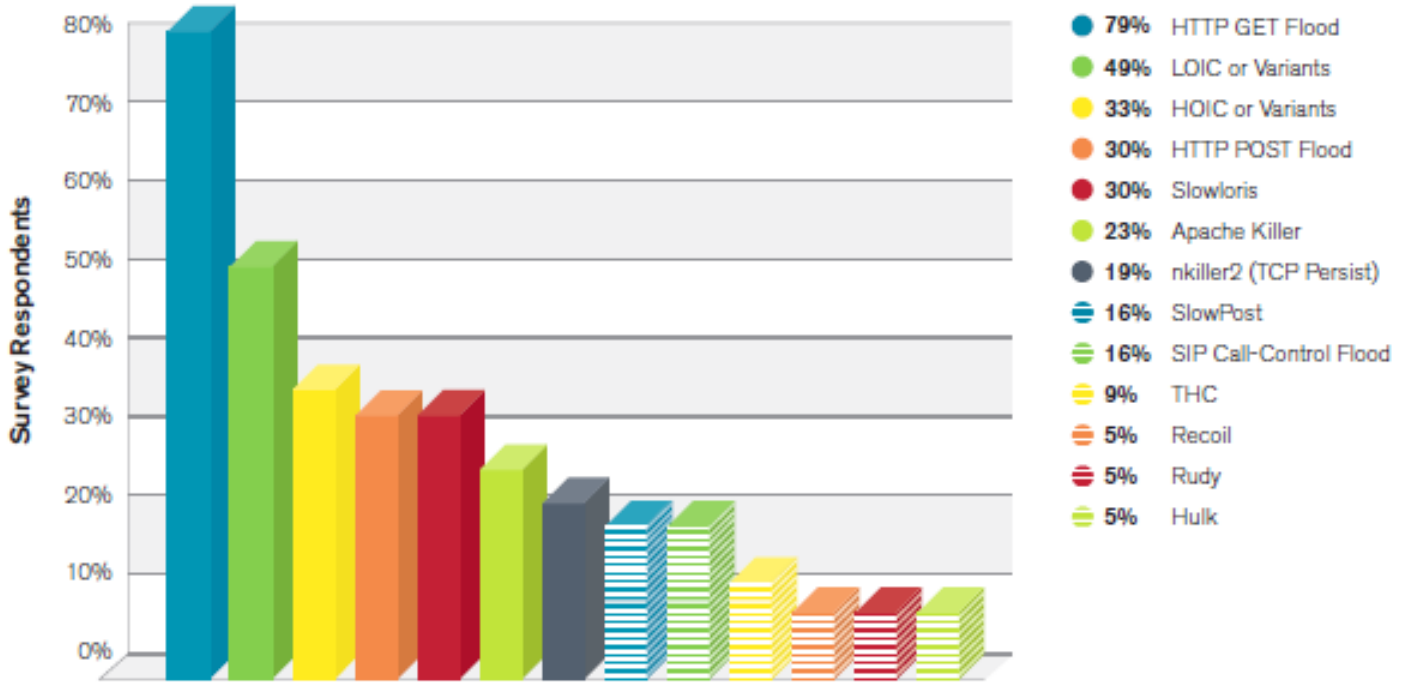


Figure 25 Source: Arbor Networks, Inc.

Multi-Vector DDoS Attacks

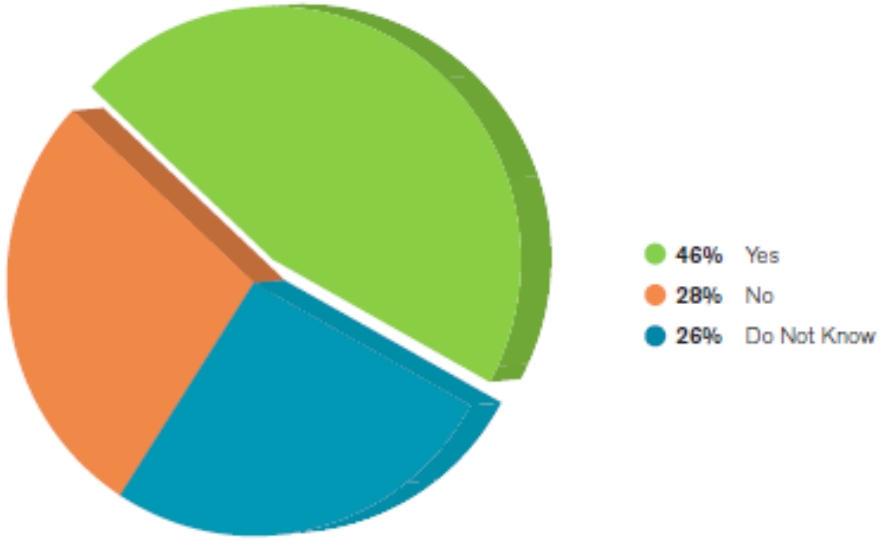
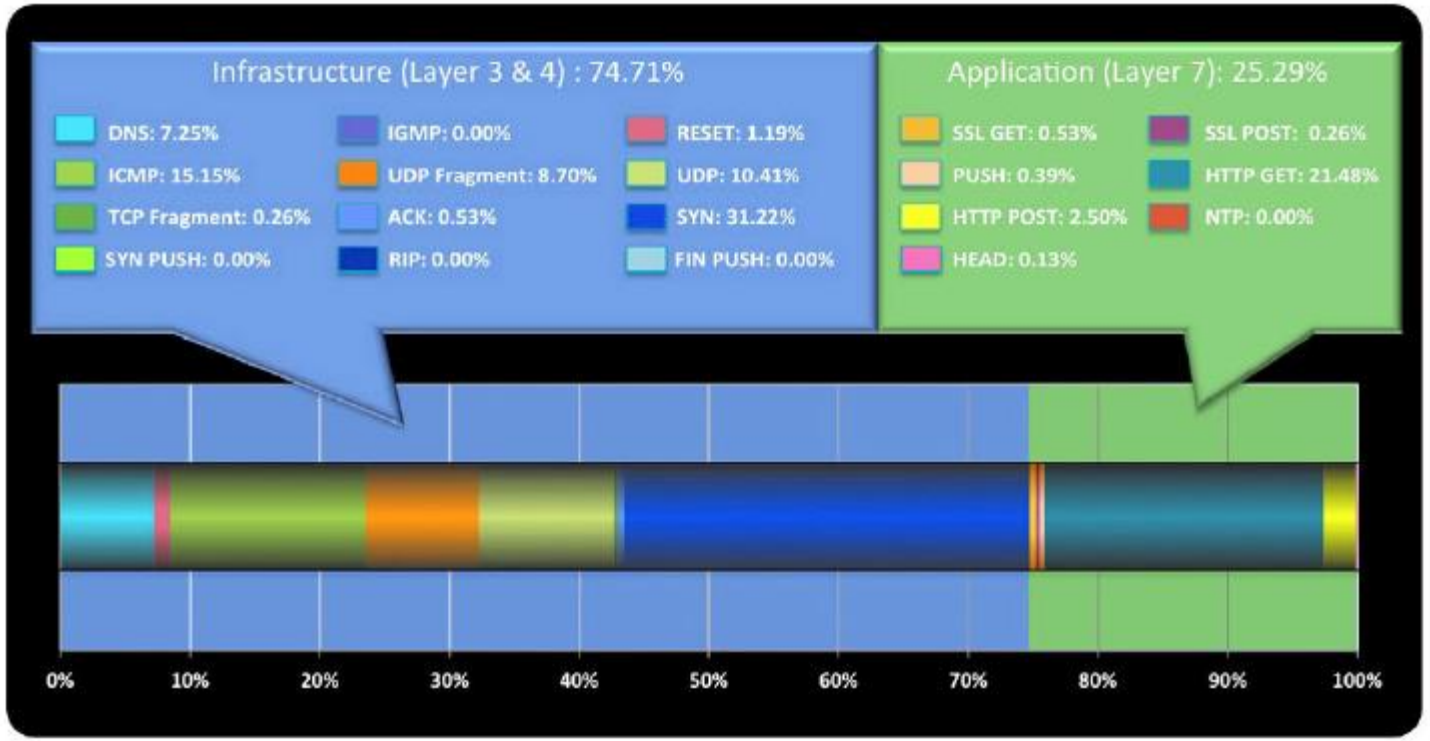


Figure 26 Source: Arbor Networks, Inc.

Arbor Worldwide Infrastructure SecurityReport 2012

How it is Being Attacked (2)



Prolexic Quarterly DDoS Attack Report Q2/2013

Defense Types

- On-Demand
  - Vendor-based mitigation
  - Route attacked address space through mitigation centre
  - ISP model
  - Expensive to sustain
- Always-on
  - On-Site appliances
  - Cloud-based CDN / WAF solution
  - Requires web site operators to understand inner workings of applications

SentryMetrics

Defending Against Protocol Attacks

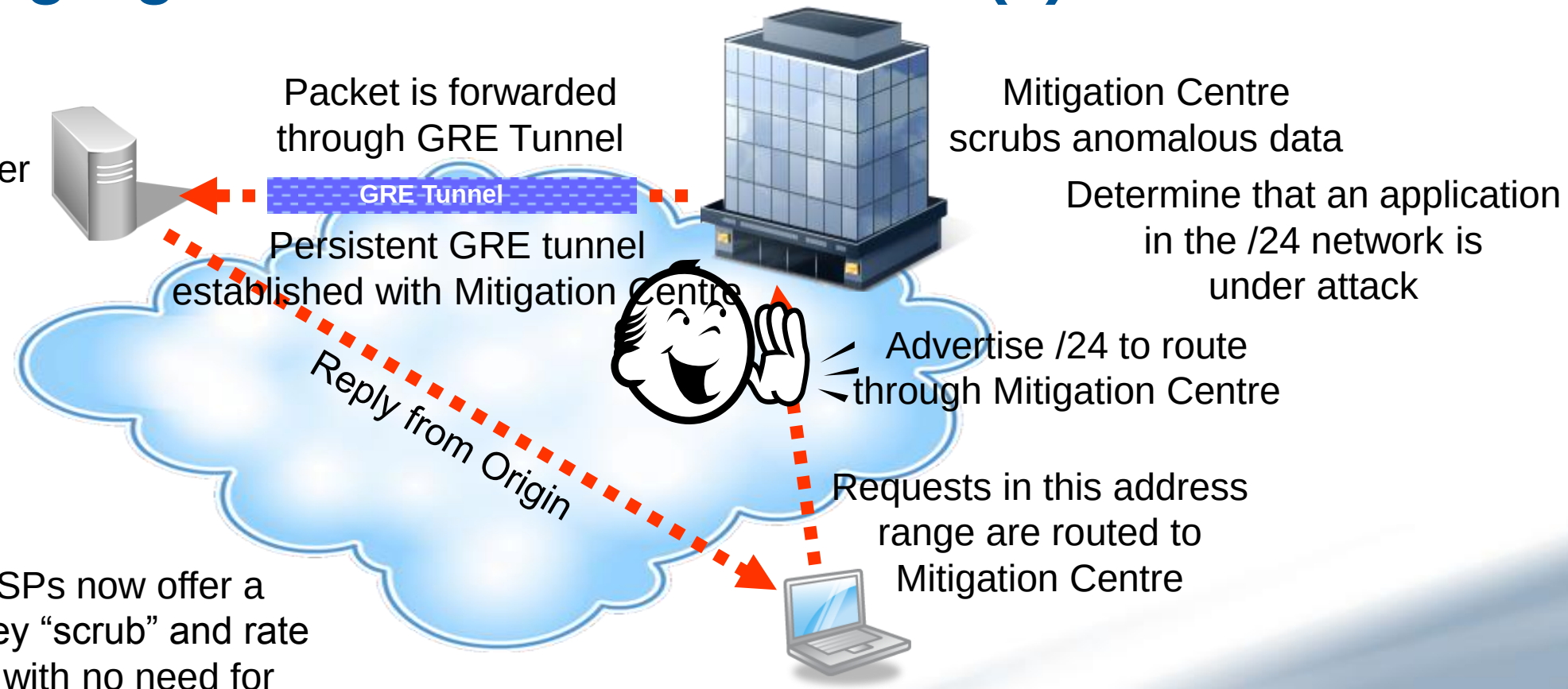
- Protocol attacks take advantage of malformed packets, or abusing design features of some protocols
- Following vendor best practices and hardening mitigate many of these attacks
- Traditional Firewall, IPS, and AV Systems will mitigate many as well
- New class of DDoS Mitigation devices such as those from Arbor, Fortinet, Radware, Cisco, A10, and others continue to evolve
- These devices are more typically used to help mitigate Volumetric Attacks

SentryMetrics

Defending Against Volumetric Attacks

- Favorite attack vector of Anonymous, LulzSec
- Also used by Syrian Electronic Army and Al-Qassam Cyber Fighters
- Typically makes use of botnets to overwhelm network bandwidth, or at least overwhelm network gear at the attack target
- DDoS Mitigation appliances can sit between the Internet and your Firewall to “scrub” or rate limit traffic
- In many cases, this is insufficient since your Internet pipe gets overwhelmed, so legitimate traffic never reaches your network
- Cloud-base scrubbing to the rescue

Defending Against Volumetric Attacks (2)



Many upstream ISPs now offer a service where they “scrub” and rate limit traffic inline, with no need for GRE tunnel

DDoS Mitigation Services – Pros and Cons

- Initial setup can take some time to get right
- Profiling “normal” traffic
- Can mitigate any protocol attacks
- Asymmetric routing ensures no added latency when sending data back to legitimate users
- Typically not “always on” since ISPs and 3rd-Parties don’t want to invest too heavily in DDoS Mitigation equipment and Bandwidth
- Downtime when an attack starts
- Provisioning SSL certificates
- Doesn’t protect against application logic attacks

SentryMetrics

Application Attacks

- Innumerable attacks:
  - HTTP Protocol, URL Encoding, Web Server Flaws, 0-Day vulnerabilities
  - Resource Consumption: Large GETs, Slow Post, SSL Handshake, Slowloris, Search Forms
  - SQL Injection, XSS, XSRF
  - Information Leakage (Error Messages, SQL Statements, IP Addresses)
- Attackers want to use as few hosts as possible to attack from since most require TCP connection
- DDoS Mitigation services have generic prevention
- Web Application Firewalls mitigate Application or Business Logic attacks

SentryMetrics

Web Application Firewalls

- WAFs are rule-based engines similar to IPS systems (RegEx) using Deep Packet Inspection (DPI) engines
- Come with generic detection typically based on modSecurity
- Custom rules can be built to match application logic
- Plan for regular tuning, as apps change and new attack patterns emerge
- Developers may need additional testing to accommodate WAF
- Always enabled security protection (more than just DDoS)
- Cloud-based and On-Premises solutions available

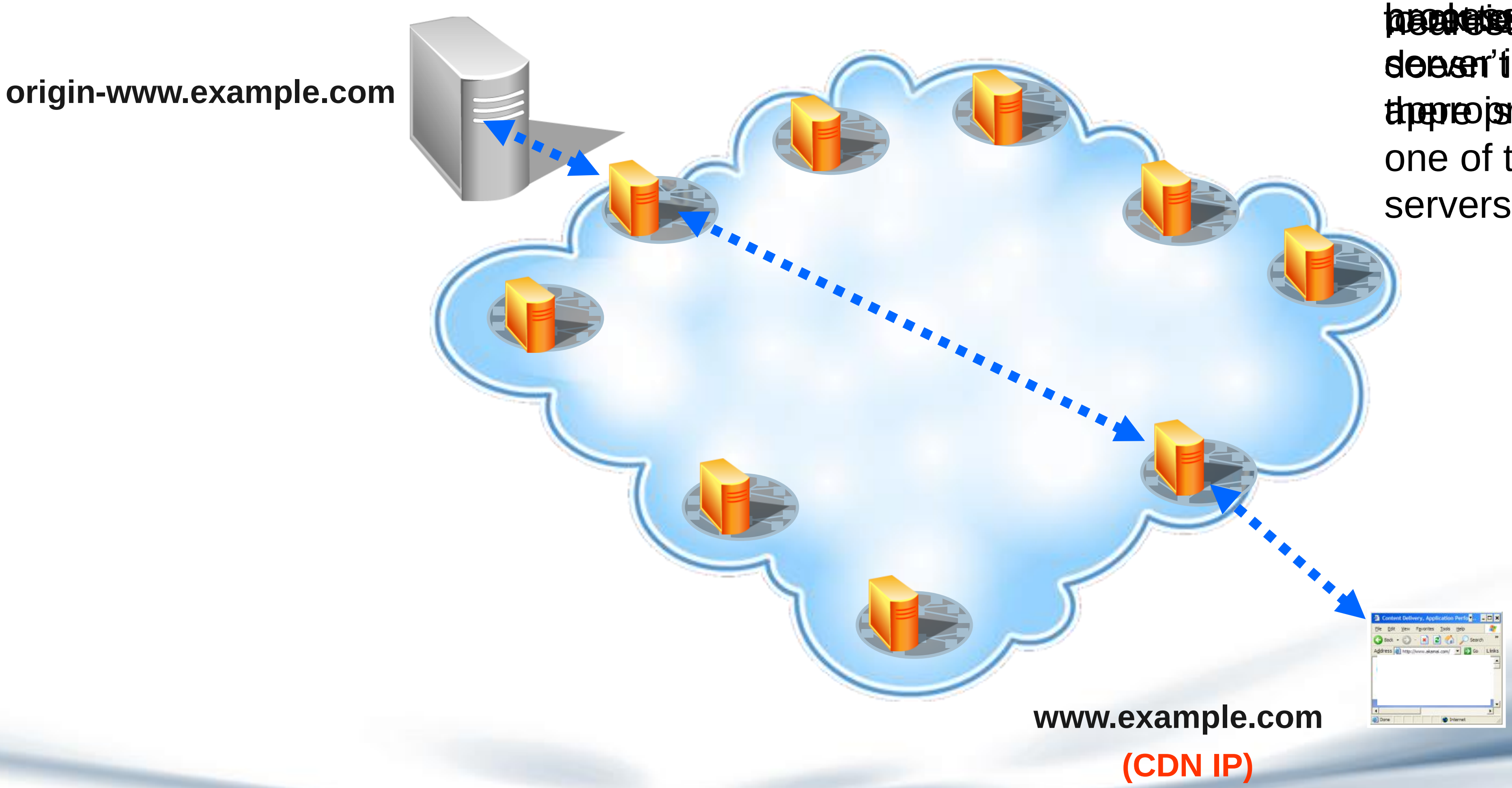
Cloud-based WAFs

- Tied to Content Delivery Networks (CDN)
- CDNs work like a reverse-proxy, caching objects, offloading 50-80% of traffic
- Cloud-based, distributed nature of CDN means less load on origin servers during Volumetric attacks
- Must provide SSL keys to CDN

Cloud-based WAFs Example

User resolves web property to nearest CDN address

If CDN server doesn't have all data cached or there is dynamic data, it queries one of the pre-defined CDN servers near origin.



Cloud-based WAFs – Pros & Cons

- Dynamic content must still return to origin servers, so attack vector remains
- Can handle much of the loads due to CDN integration
- Protects against HTTP(S) attacks only (not DNS, FTP, SMTP, etc.)
- Requires providing SSL cert to vendor
- Attackers can still target origin directly, unless ACLs are put in place
- “Spaghetti” calls between apps or out to Internet
- App developers need to understand caching rules and web logic
- Help mitigate self-inflicted DDoS attacks - successful marketing campaign

On-Prem WAFs

- Not tied to CDN, so no data offloading
- Sits behind the firewall inside your network
- Doesn’t protect against Volumetric attacks
- SSL Keys are always in your control
- WAF can be used for internal applications (open networks)

Non-Web Firewall Solutions

- Still many cloud-based solutions
  - Outsourced DNS, SMTP, SIP / Chat (?)
- Typical pros/cons are feature sets
  - Intelligent DNS Load Balancing
  - Rejecting SMTP / SIP message by destination
- Increase in DNS Firewalls

Summary

- DDoS Mitigation is easier in the cloud before touching your Internet link
- Volumetric attacks against non-HTTP(S) are mitigated by DDoS Network Scrubbers
- Application layer attacks are best mitigated by WAFs (or other firewalls), and can also help harden applications (especially older ones) against attack
- Cloud based WAFs are often tied to CDNs, which can add business value
- As with most cloud technologies, they're still evolving – don't expect a static environment.

Summary - Recommendations

- Have an attack plan - What is most important to you?
- Ensure you have Professional Services engaged
- Think about splitting Web Services onto separate

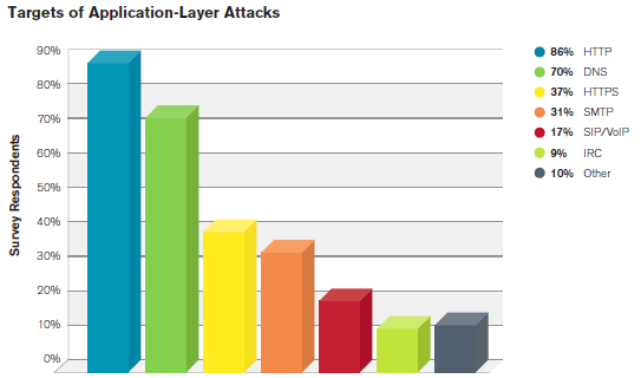


Figure 24 Source: Arbor Networks, Inc.

Arbor Worldwide Infrastructure SecurityReport 2012

link from other protocols if your business is eCommerce based

- If cloud, ask about vuln scanning or pen testing while using services
- Make sure your contract allows for protection of apps hosted by 3rd-party provider
- Ask critical service providers about their level of DDoS Protection

Questions?

SentryMetrics

the right solution at the right time.