Growing sophistication of DDoS

John Ellis, Enterprise Security Director, Akamai Technologies

The battleground

70%	5
50%	Application attacks
20Gbps	Average for DDoS
24hours	Duration of average attack
UDP 53 / TCP SSL	Achilles' heel
15x	..uses more than attacker

In the beginning ‘he’ made Trin00

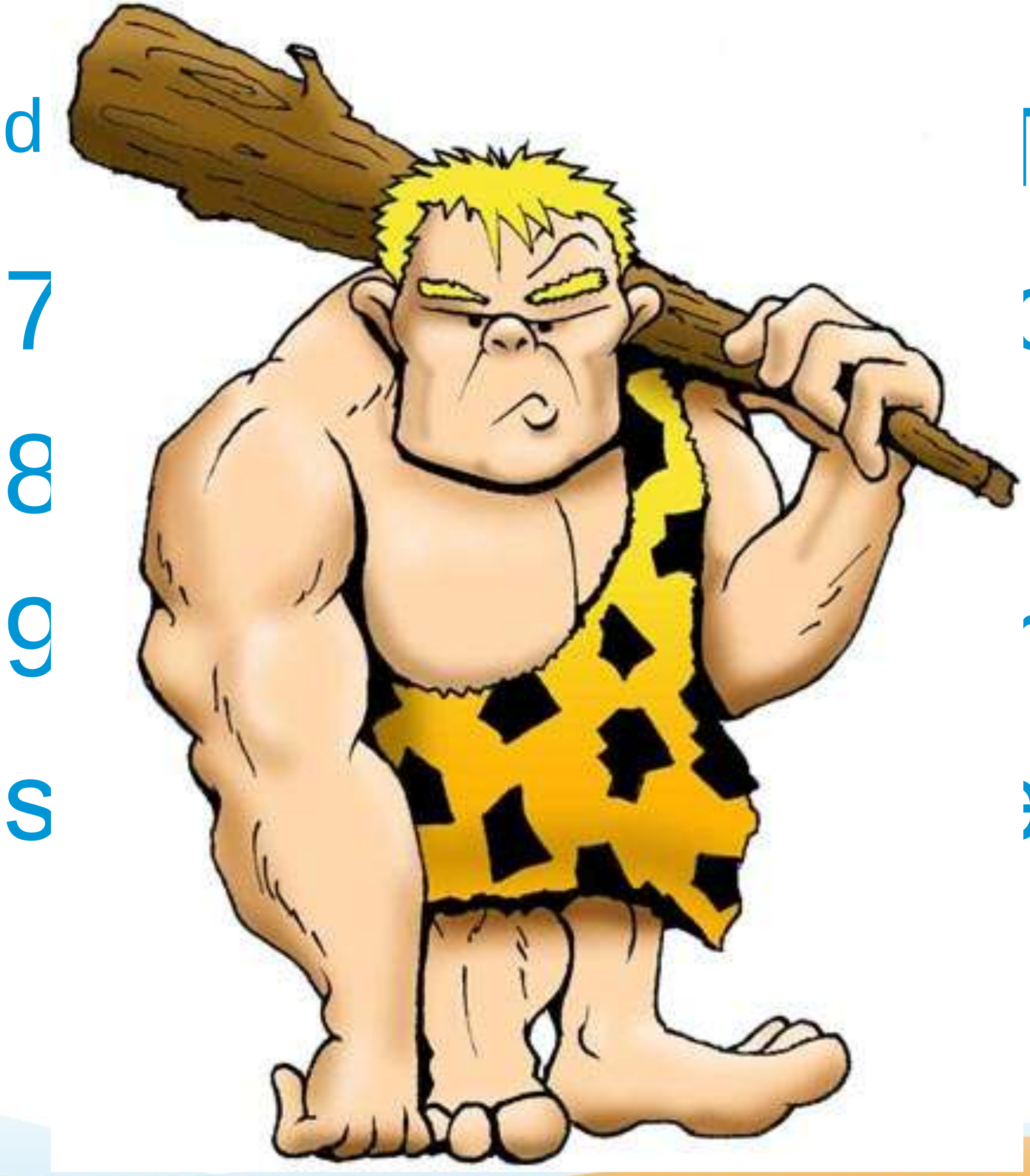
July 22nd Note 99-04

February 7 oo attacked

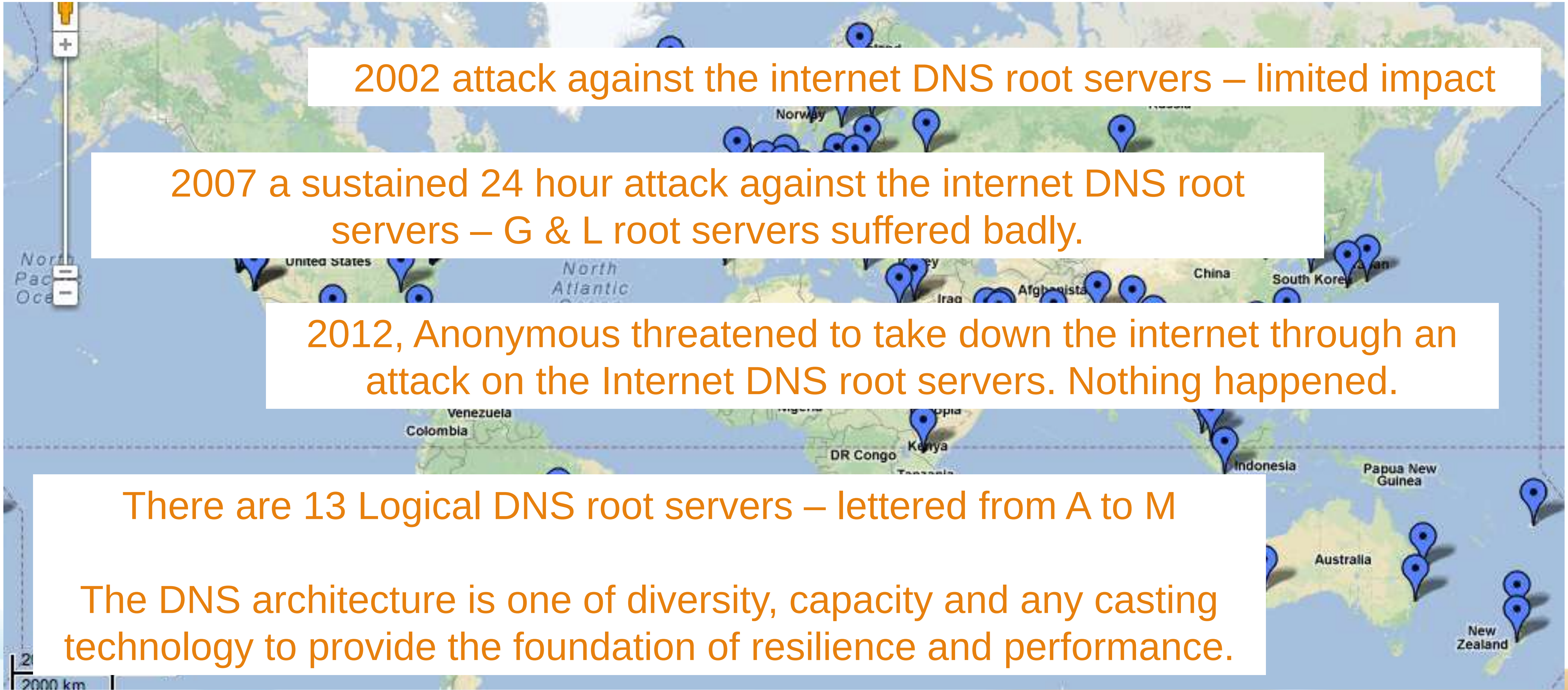
February 8 n, CNN, eBay

February 9 rade, Zdnet

Cheap, nas ective…. ☹



What’s in a name? Let’s get to the root!



2002 attack against the internet DNS root servers – limited impact

2007 a sustained 24 hour attack against the internet DNS root servers – G & L root servers suffered badly.

2012, Anonymous threatened to take down the internet through an attack on the Internet DNS root servers. Nothing happened.

There are 13 Logical DNS root servers – lettered from A to M

The DNS architecture is one of diversity, capacity and any casting technology to provide the foundation of resilience and performance.

You can call me Boris and I have bots baby…

2004

Multibet Australia

Threatened by Russians

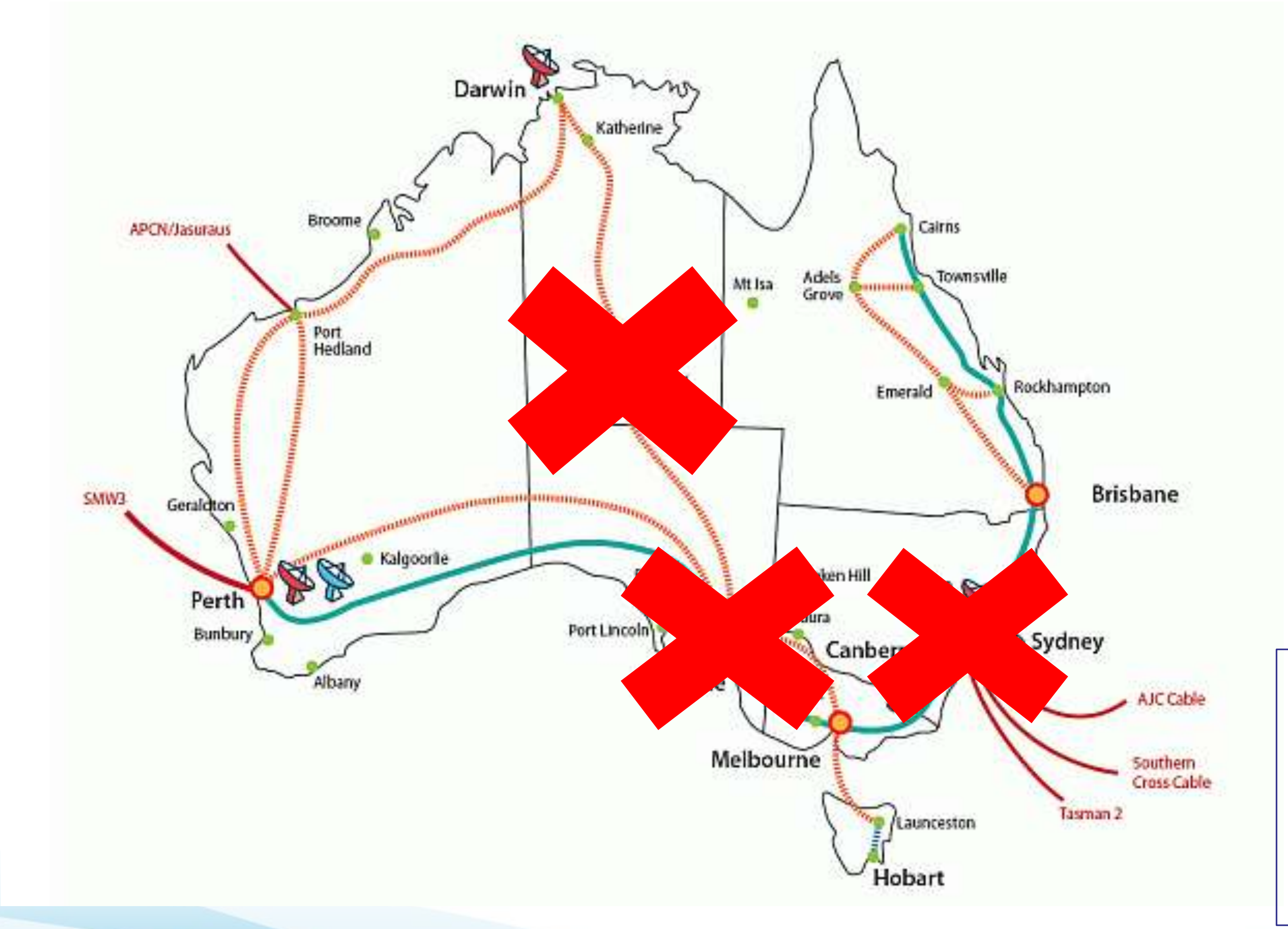
Suffered DDoS attack

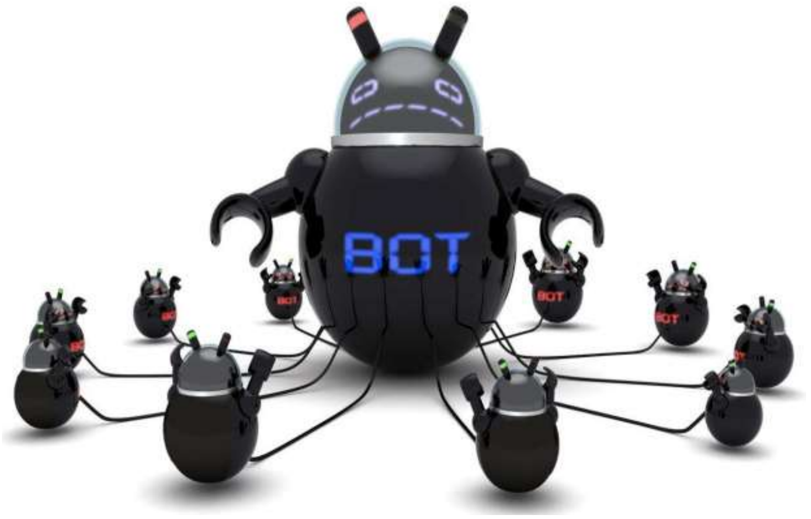
Paid $25,000

Telco said ….

No worries mate

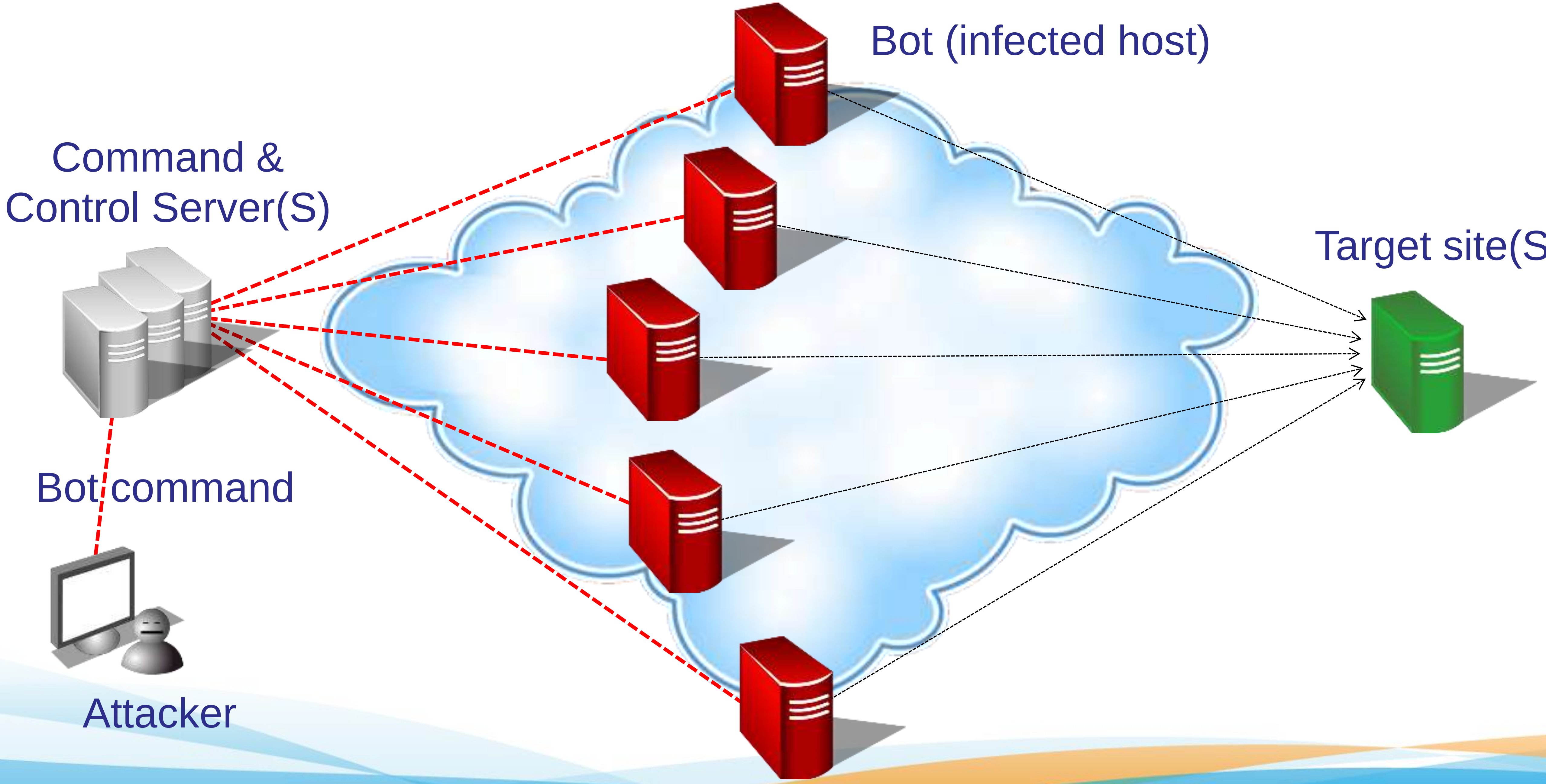
You can call me Boris and I have bots baby…



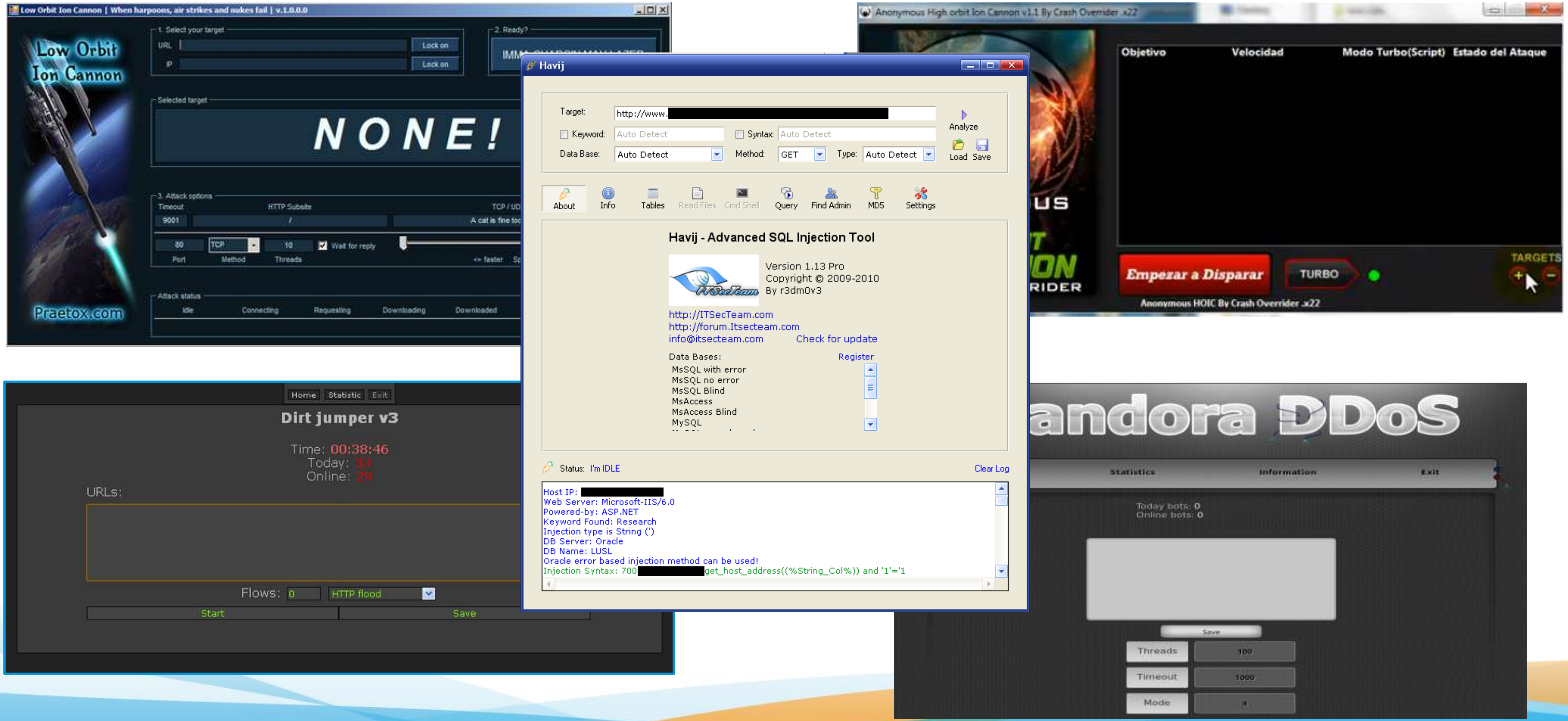


```
if source IP equals Australian IP then
            accept
Else
            deny
```

Simple C2 architecture back then



First the script kiddie, now the bot-kiddie



Havij

Target: http://www.[redacted]

☐ Keyword: Auto Detect ☐ Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Havij - Advanced SQL Injection Tool

Version 1.13 Pro
Copyright © 2009-2010
By r3dm0v3

http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com Check for update

Data Bases: Register

MsSQL with error
MsSQL no error
MsSQL Blind
MsAccess
MsAccess Blind
MySQL

Status: I'm IDLE Clear Log

```
Host IP: [redacted]
Web Server: Microsoft-IIS/6.0
Powered-by: ASP.NET
Keyword Found: Research
Injection type is String (')
DB Server: Oracle
DB Name: LUSL
Oracle error based injection method can be used!
Injection Syntax: 700[redacted]get_host_address((%String_Col%)) and '1'='1
```

Dirt jumper v3

Time: 00:38:46
Today: 33
Online: 29

URLs:

Flows: 0 HTTP flood

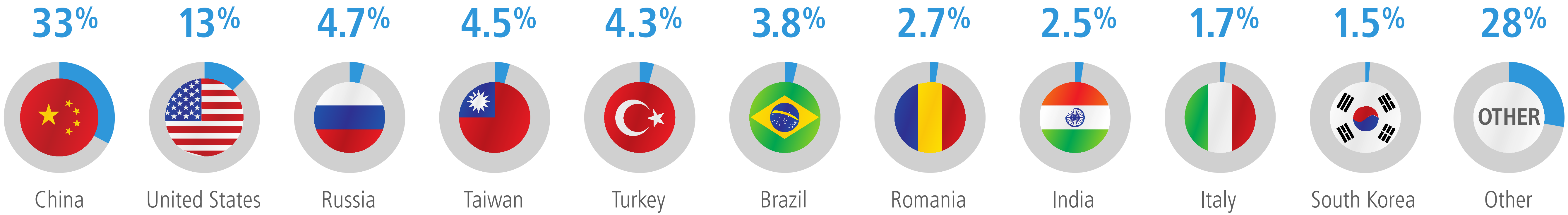
Today bots: 0
Online bots: 0

Threads 100
Timeout 1000
Mode 4

Source of attack traffic – as seen by Akamai

SECURITY: ATTACK TRAFFIC

Nearly 51% of observed attack traffic originated in the Asia Pacific/Oceania region, while just over 23% originated in North and South America and just under 25% originated in Europe. The remaining 1% of attack traffic originated in Africa.



● *The blue areas represent each country's percentage of the overall total amount of attack traffic observed by Akamai.*

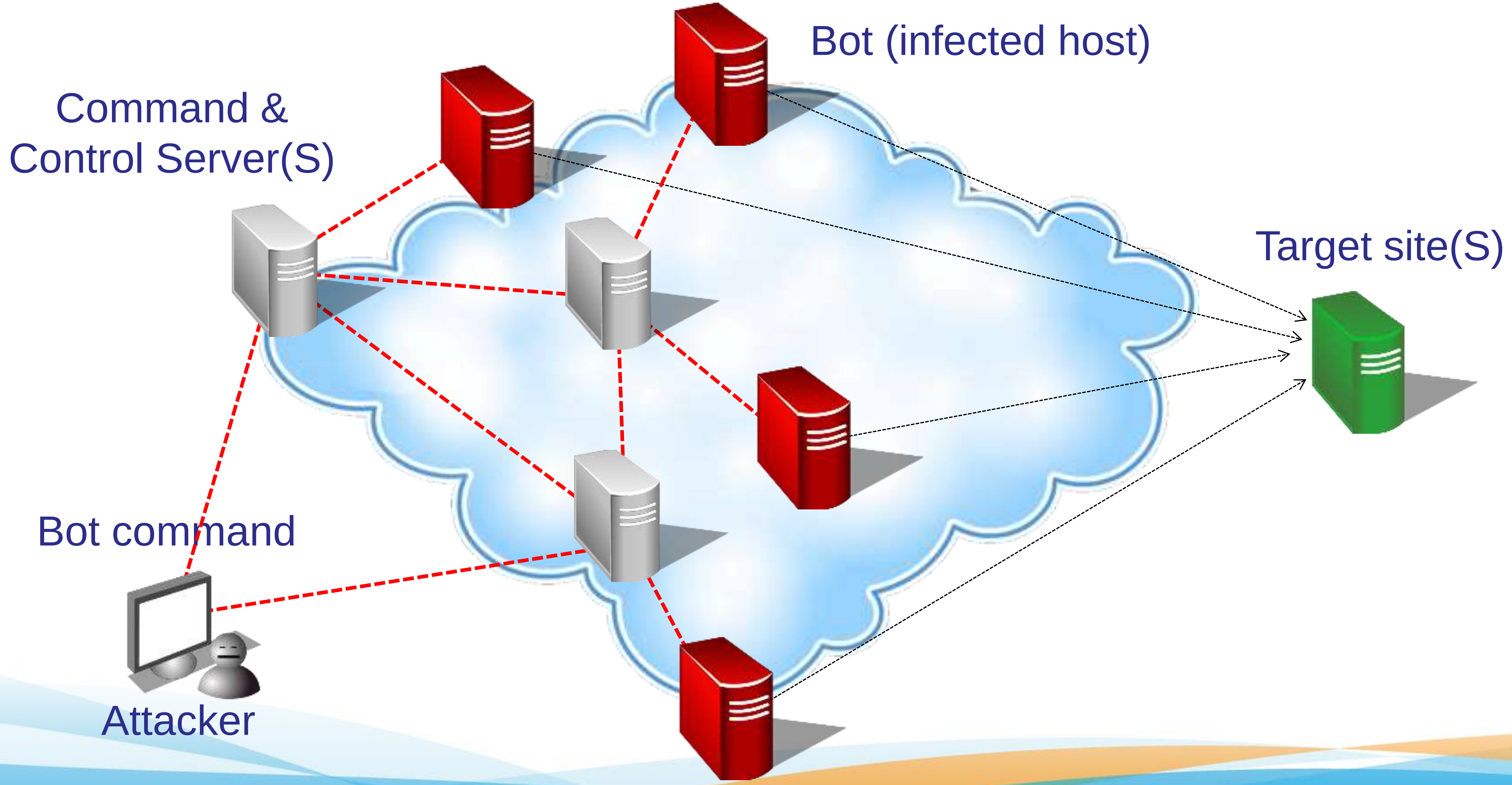
Operation Ababil – Financial Service DDoS

- 18 September 2012 ‘Cyber fighters of Izz ad-in Al qassam’ called on hacktvists to join-in a cyber campaign against American FSI
- Multistage campaign attacking a number of major FSIs such as NYSE, BoA, JPMC
- Akamai saw attack traffic in excess 65Gbps
- Initial campaign lasted for five days in which all targets experienced significant service disruption

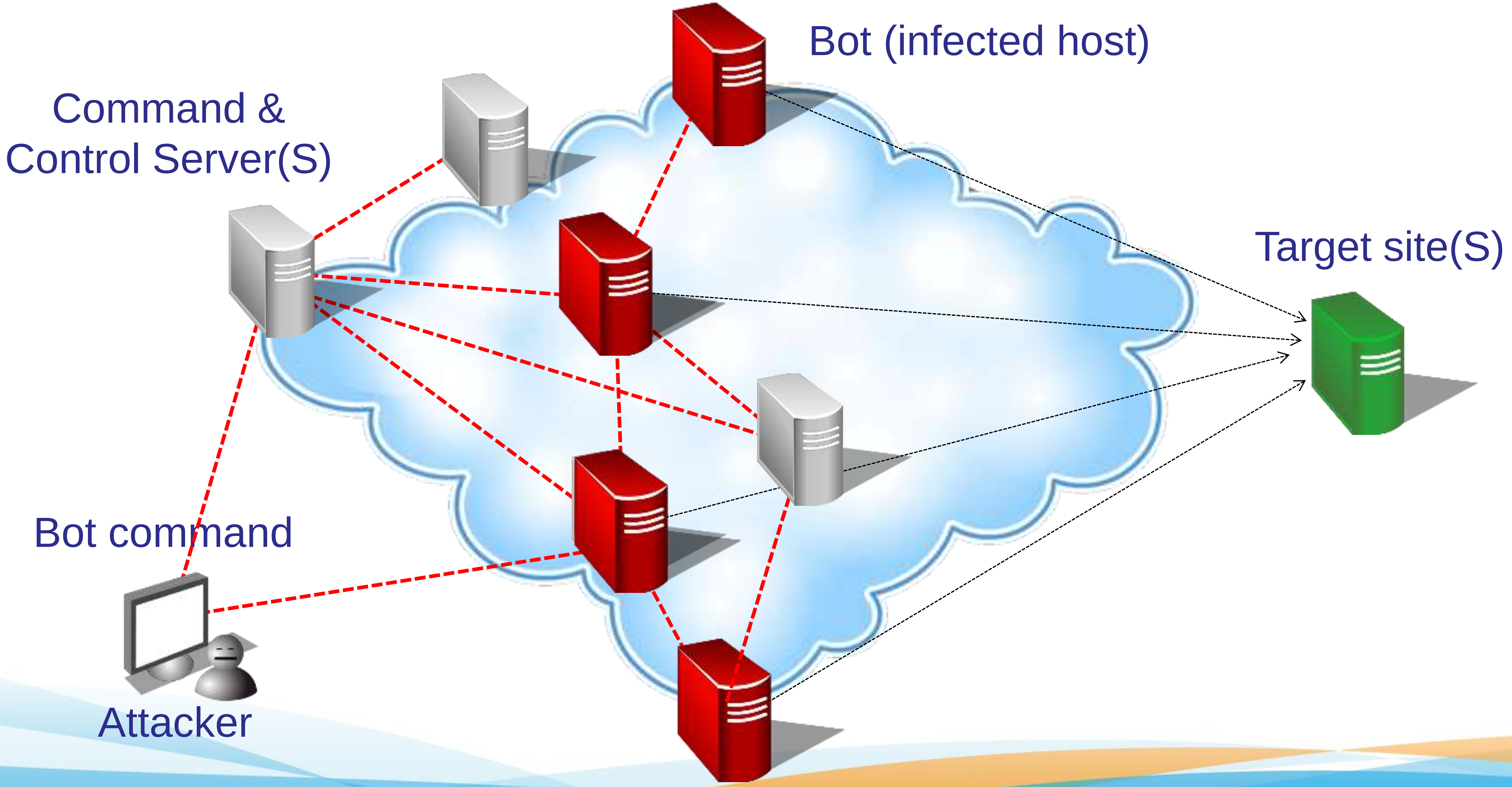
Some interesting observations (the technical stuff)

- Use
- Use
- Boo
- Traf
- 700
- Sim
- Qui

‘itsoknoproblembro’ C2 architecture

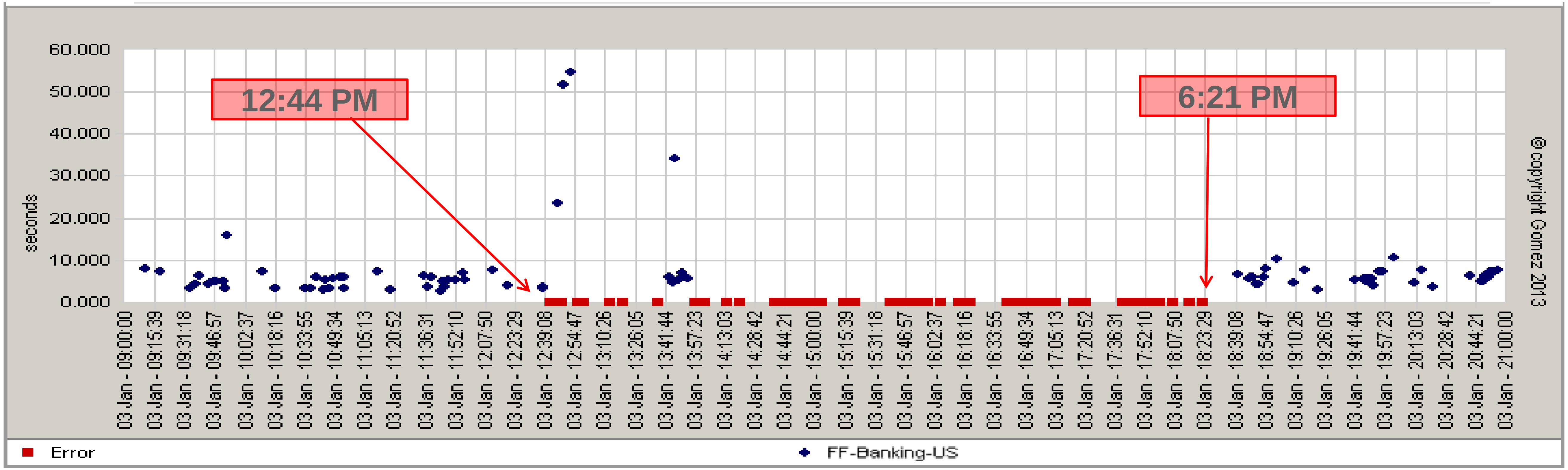


‘itsoknoproblembro’ C2 architecture



US bank attacked at 12:44 PM 03 January 2013

- Gomez benchmark of bank home page, measured from 12 cities 1x per hour.
- First outage recorded at 12:44 PM.
- Attack continued to 6:21 PM.



Traditional mindset in dealing with DDoS

Deploy significant capacity in the data center ……to

absorb ‘flash’ crowds and peaks in high traffic loads

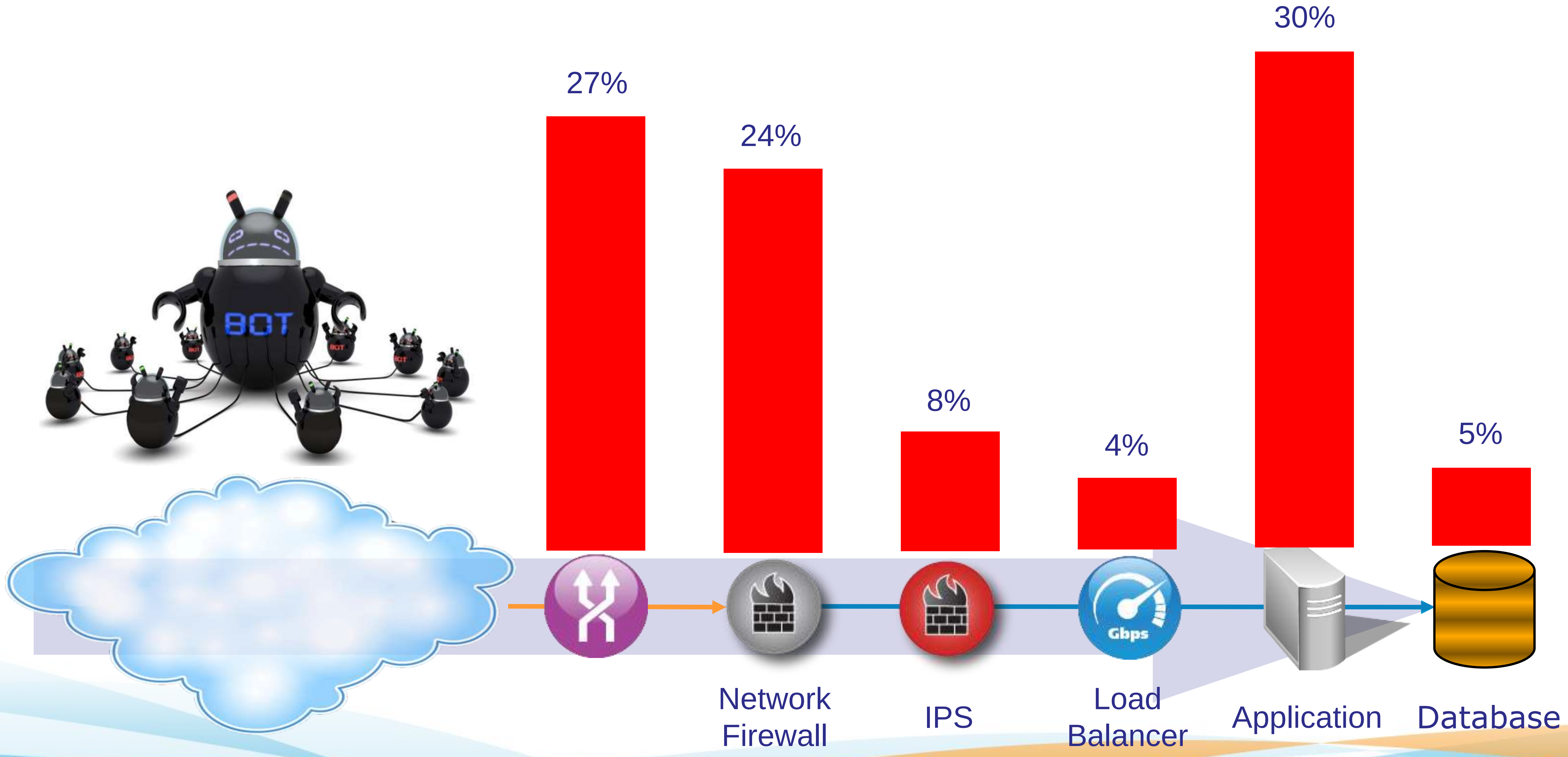
Leverage network security defenses like firewalls, intrusion prevention systems, and load balancers……...to

inspect, filter, and manage network traffic

Engage with Internet service provider for…….

a ‘clean’ pipe service or ‘scrubbing’ service

But we built this city on firewalls



What happened? Why did so many banks struggle?

Deploy significant capacity in the data center to absorb ‘flash’ crowds and peaks in high traffic loads

Leverage network security defenses like firewalls, intrusion prevention systems, and load balancers to inspect, filter, and manage network traffic

Engage with Internet service providers for a ‘clean’ pipe service or ‘scrubbing’ service

Often targets of the attacks and have limited capacity to deal with sizeable attacks.

Increased cost, addresses less than 40% of DDoS attacks

Clean pipe solutions offer limited protection. Still places significant strain of perimeter defenses.

Observations, and things to ponder

How must our security protections evolve to get and stay ahead of the rapid changes?

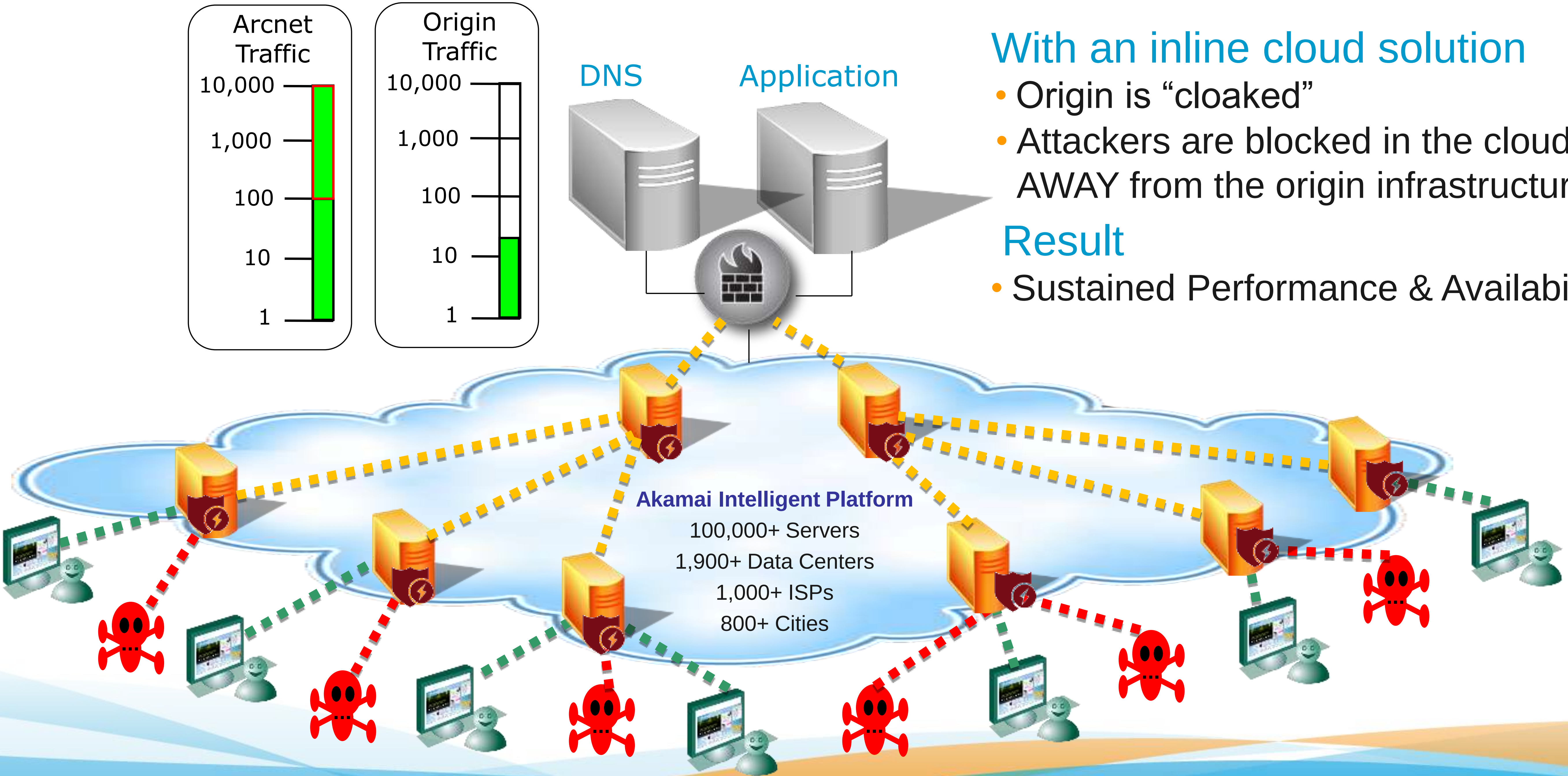
How can we be more resilient to attacks, whilst containing costs?

My online platforms need to perform irrespective if they are under attack.

Solutions need to deliver real-time protection, and not wait for ‘people’ to determine what to do next.

the arc net

Do we need K to deploy the arcnet?



With an inline cloud solution

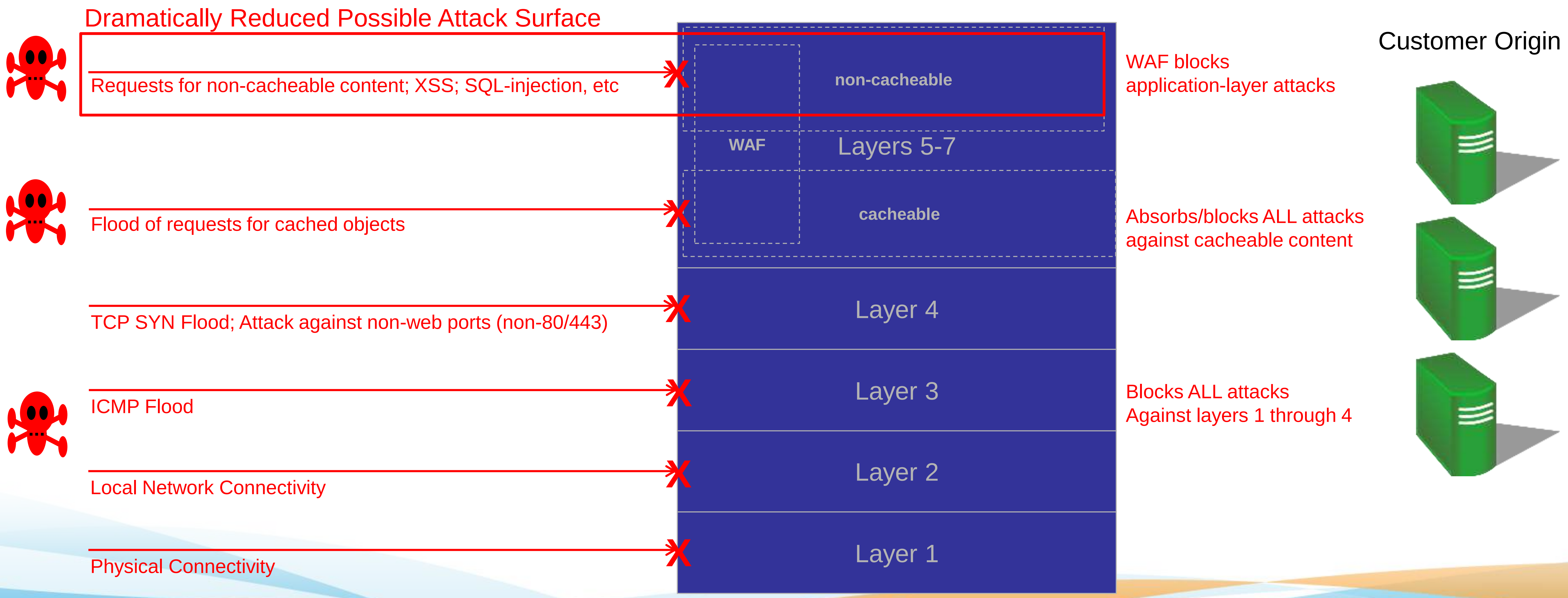
- Origin is “cloaked”
- Attackers are blocked in the cloud, AWAY from the origin infrastructure

Result

- Sustained Performance & Availability

Protect ALL Layers of the OSI stack

Multi-Layered Defense



Dramatically Reduced Possible Attack Surface

Requests for non-cacheable content; XSS; SQL-injection, etc

Flood of requests for cached objects

TCP SYN Flood; Attack against non-web ports (non-80/443)

ICMP Flood

Local Network Connectivity

Physical Connectivity

non-cacheable

WAF

Layers 5-7

cacheable

Layer 4

Layer 3

Layer 2

Layer 1

WAF blocks application-layer attacks

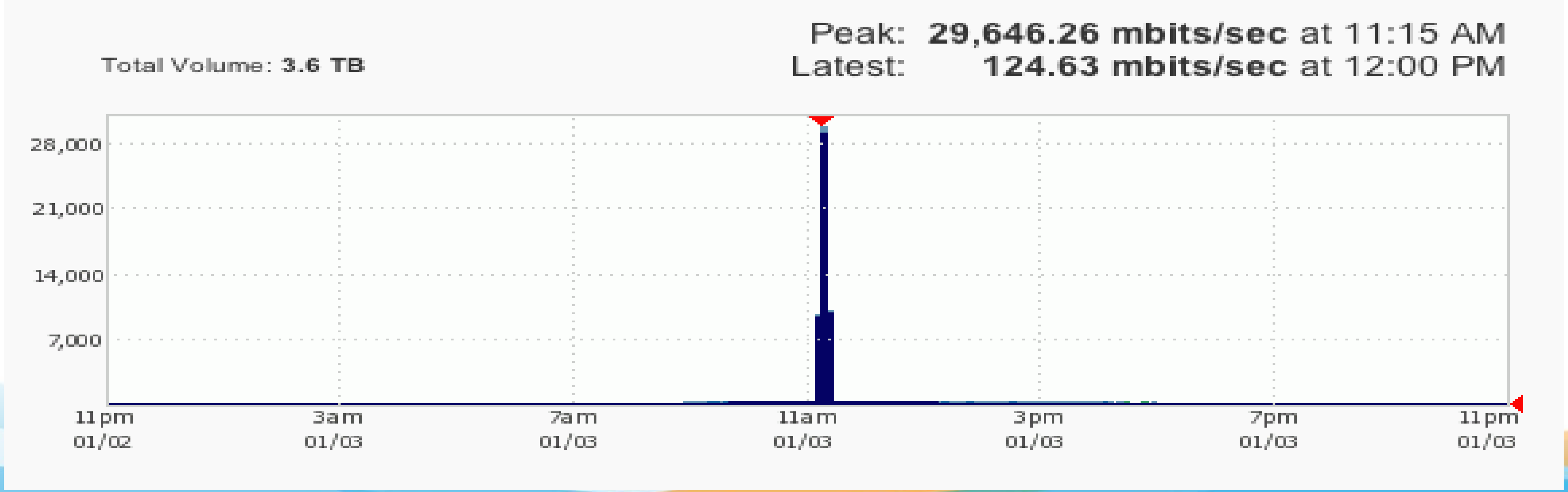
Absorbs/blocks ALL attacks against cacheable content

Blocks ALL attacks Against layers 1 through 4

Customer Origin

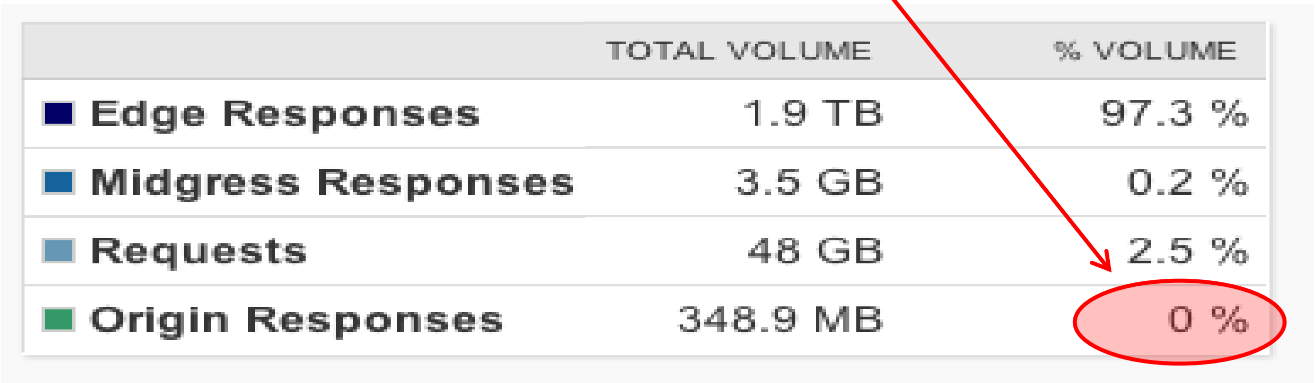
A bank that used a Cloud ‘arcnet’ solution *Always on Protection*

- Top financial services firm with nearly 10M customers.
- Peak attack traffic was 30 Gbps, 30x normal daily high traffic.
- Attackers gave up after 15 minutes, and moved attack to another bank.
- 100% of the attack was on SSL.

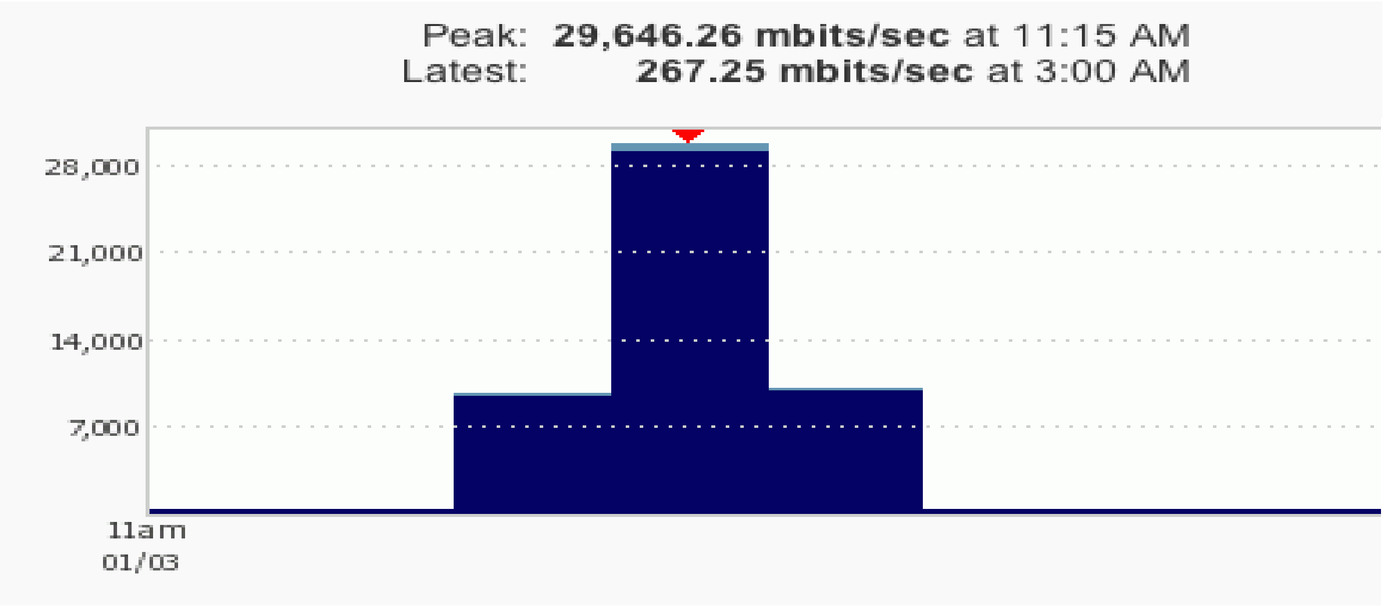


Massive Banking DDoS Attack

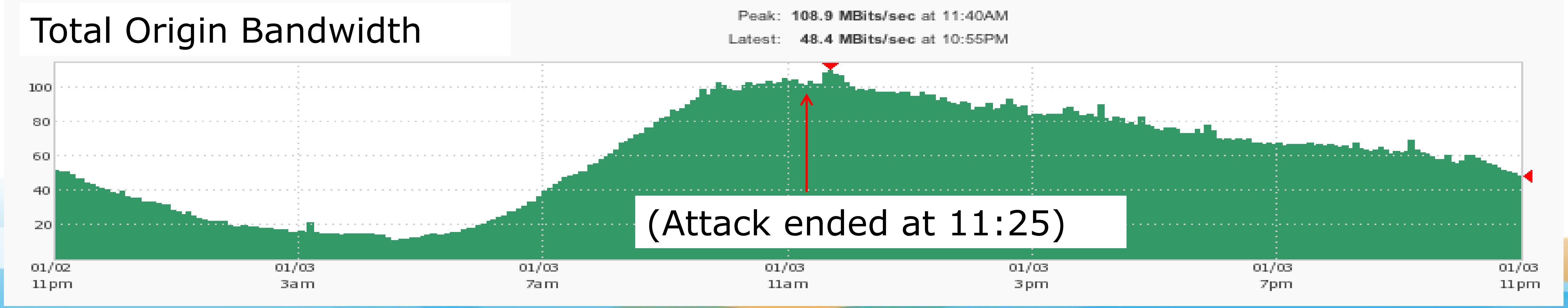
- Akamai offloaded 100% of the attack.



	TOTAL VOLUME	% VOLUME
■ Edge Responses	1.9 TB	97.3 %
■ Midgress Responses	3.5 GB	0.2 %
■ Requests	48 GB	2.5 %
■ Origin Responses	348.9 MB	0 %



- A bug impacting our windshield”.

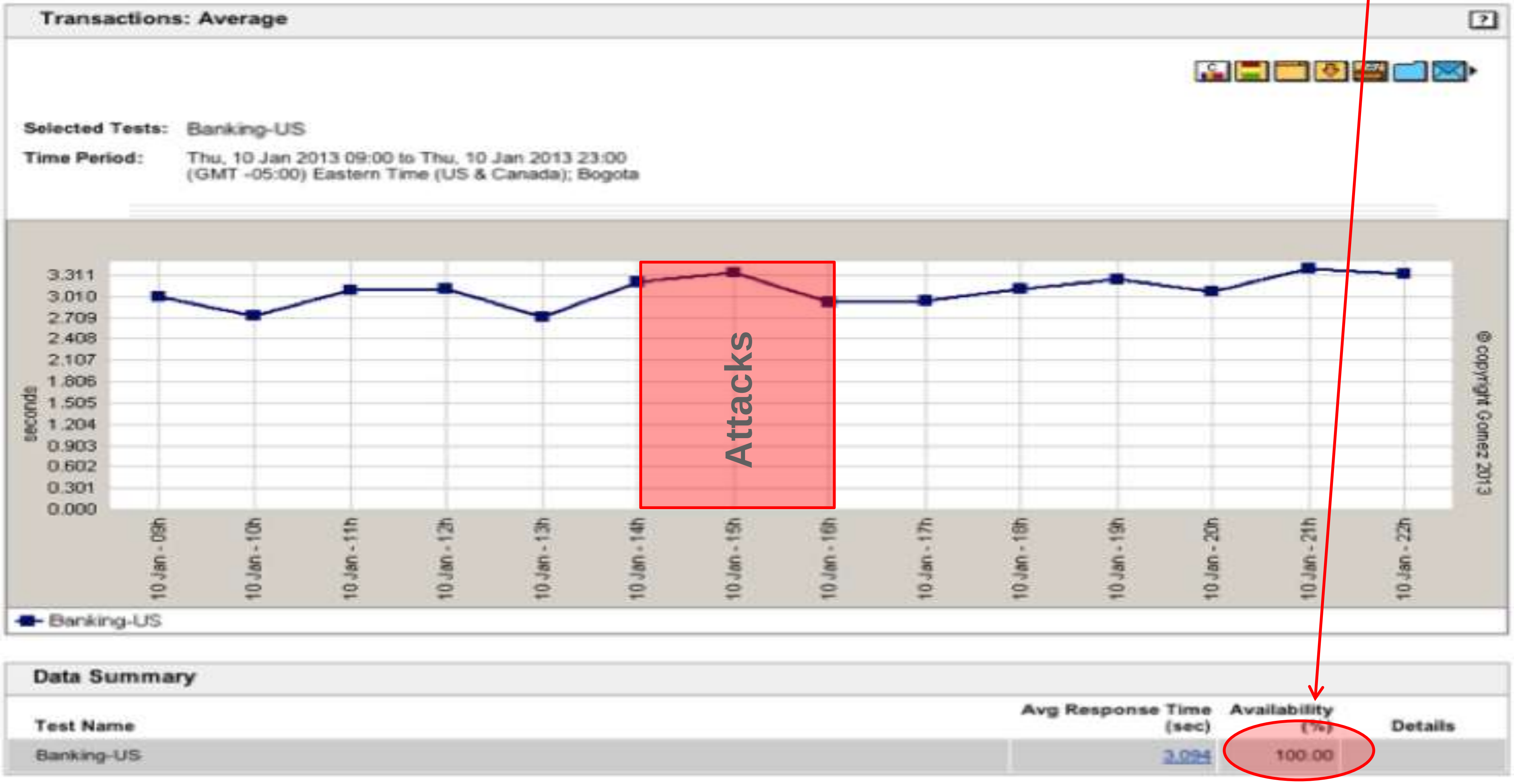


Total Origin Bandwidth

(Attack ended at 11:25)

And Perform….you must

- Gomez banking benchmark for this site. 12 U.S. measurement agents.
- No performance impact during this attack. 100% availability.   No outliers.



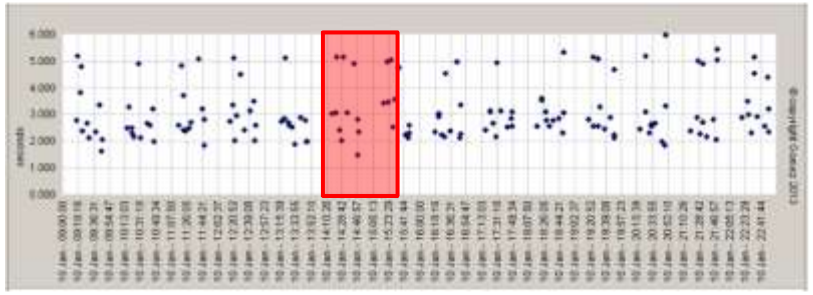
Transactions: Average

Selected Tests: Banking-US

Time Period: Thu, 10 Jan 2013 09:00 to Thu, 10 Jan 2013 23:00
(GMT -05:00) Eastern Time (US & Canada); Bogota

Data Summary

Test Name	Avg Response Time (sec)	Availability (%)	Details
Banking-US	3.094	100.00	



Before we say goodbye….

….what alternative is there to the internet?

Innovation is vital to capitalizing the opportunities

The internet has inherit issues with performance and security

You can make the internet work for you…..

….protect your investment, succeed even when under attack

….move closer to your users and the attackers, accelerate the good, block the bad