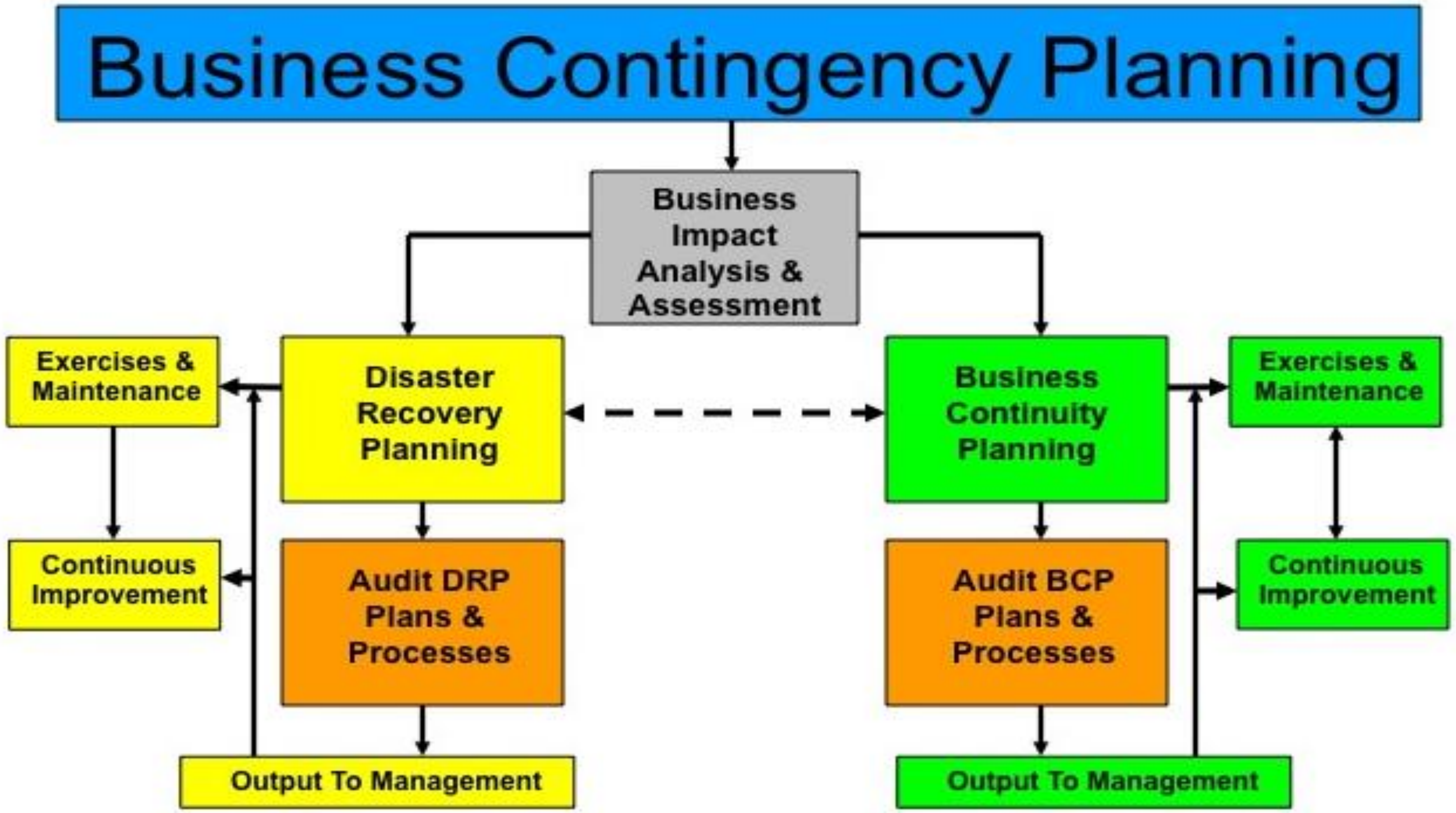
Akamai FASTER FORWARD

Cloud Security In Your Contingency Plans

Jerry Lock

Security Sales Lead, Greater China

Contingency Plans



Business Contingency Planning

Business Impact Analysis & Assessment

Disaster Recovery Planning

Business Continuity Planning

Exercises & Maintenance

Continuous Improvement

Audit DRP Plans & Processes

Audit BCP Plans & Processes

Output To Management

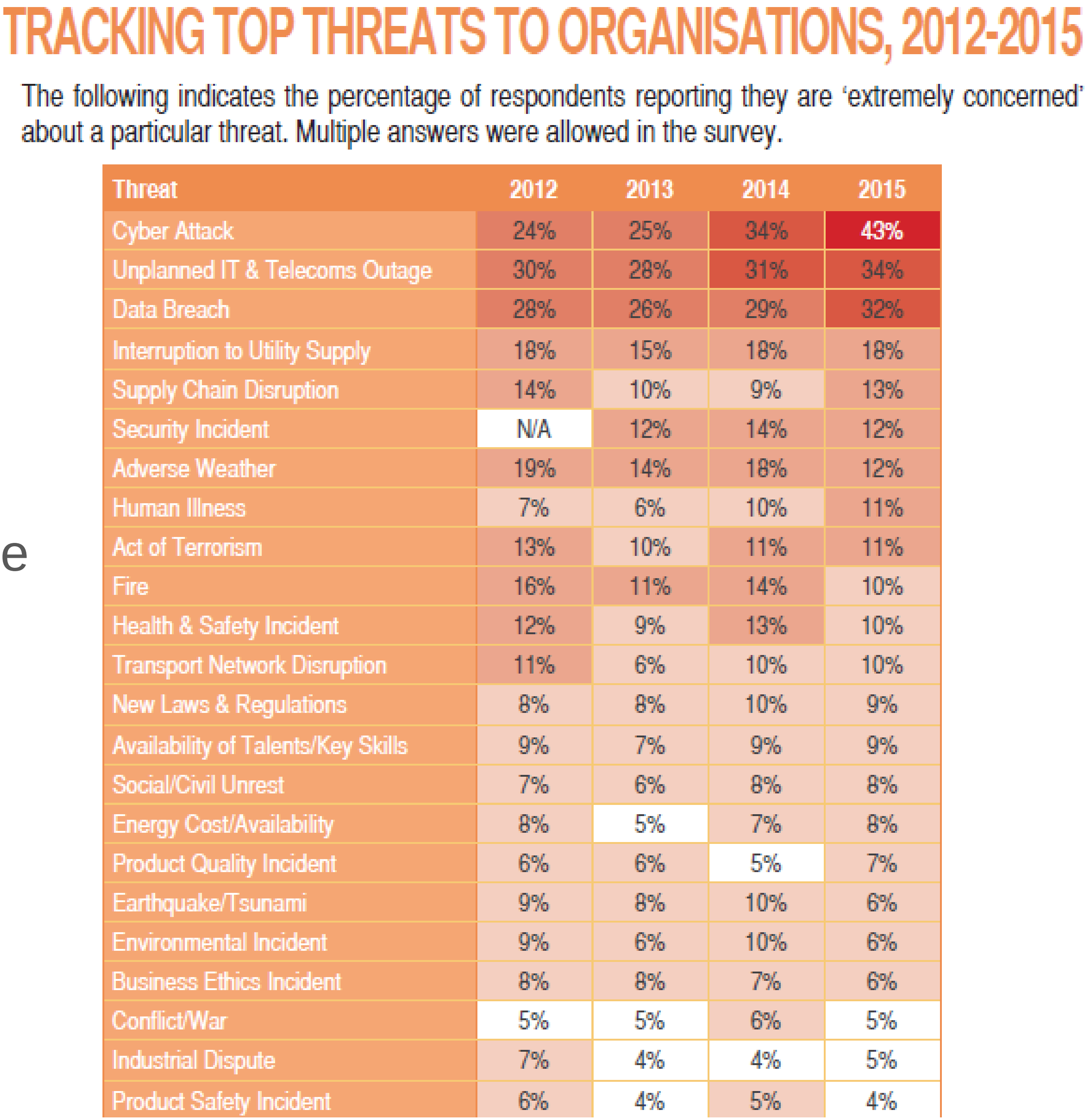
Exercises & Maintenance

Continuous Improvement

Output To Management

- Disaster Recovery Plan (IT)
- Business Continuity Plan
- Business Impact Analysis
- Exercises & Maintenance

Top Threats (2012 – 2015)



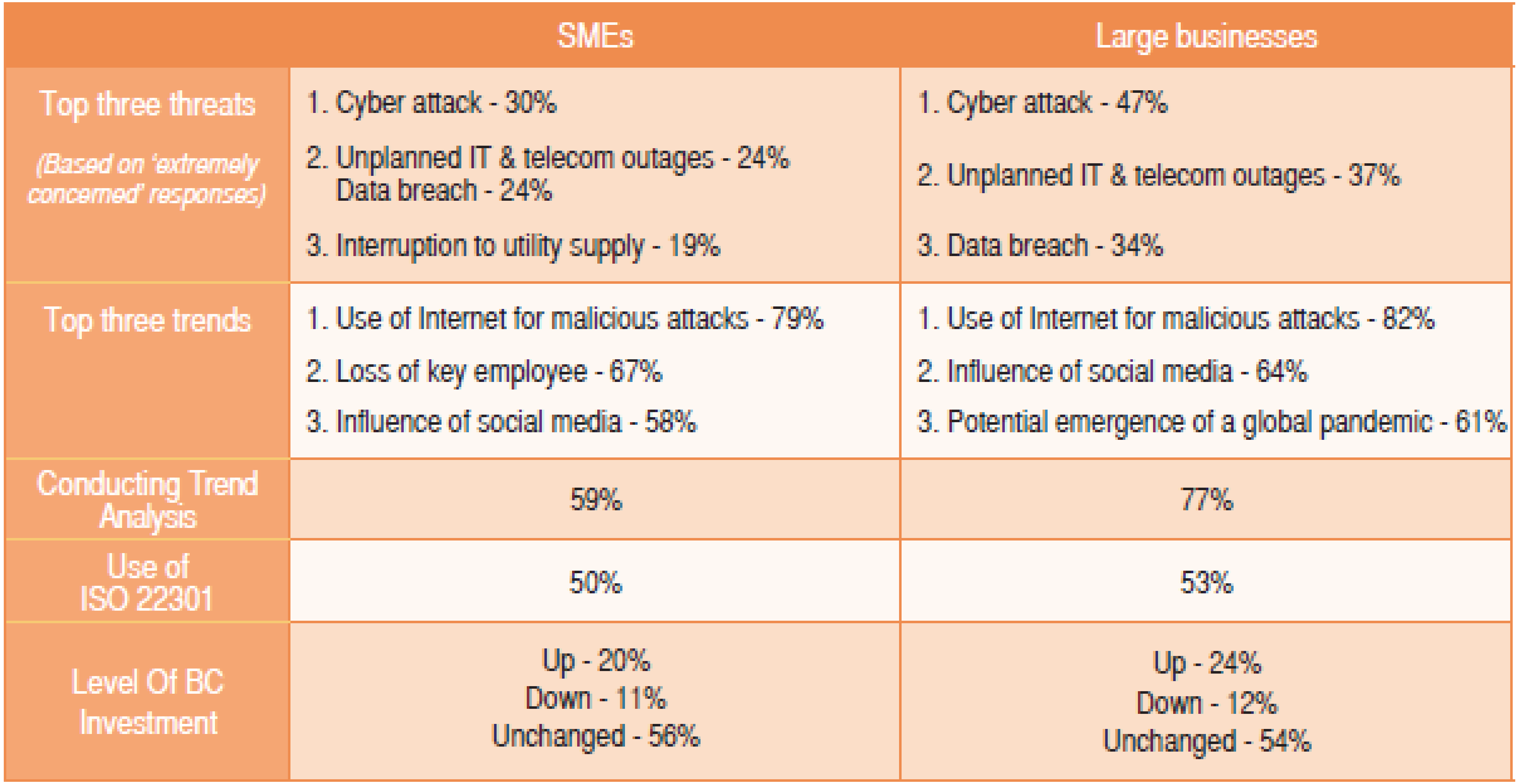
TRACKING TOP THREATS TO ORGANISATIONS, 2012-2015

The following indicates the percentage of respondents reporting they are ‘extremely concerned’ about a particular threat. Multiple answers were allowed in the survey.

Threat	2012	2013	2014	2015
Cyber Attack	24%	25%	34%	43%
Unplanned IT & Telecoms Outage	30%	28%	31%	34%
Data Breach	28%	26%	29%	32%
Interruption to Utility Supply	18%	15%	18%	18%
Supply Chain Disruption	14%	10%	9%	13%
Security Incident	N/A	12%	14%	12%
Adverse Weather	19%	14%	18%	12%
Human Illness	7%	6%	10%	11%
Act of Terrorism	13%	10%	11%	11%
Fire	16%	11%	14%	10%
Health & Safety Incident	12%	9%	13%	10%
Transport Network Disruption	11%	6%	10%	10%
New Laws & Regulations	8%	8%	10%	9%
Availability of Talents/Key Skills	9%	7%	9%	9%
Social/Civil Unrest	7%	6%	8%	8%
Energy Cost/Availability	8%	5%	7%	8%
Product Quality Incident	6%	6%	5%	7%
Earthquake/Tsunami	9%	8%	10%	6%
Environmental Incident	9%	6%	10%	6%
Business Ethics Incident	8%	8%	7%	6%
Conflict/War	5%	5%	6%	5%
Industrial Dispute	7%	4%	4%	5%
Product Safety Incident	6%	4%	5%	4%

--Business Continuity Institute Horizon Scan Report 2015

Comparison by Business Size



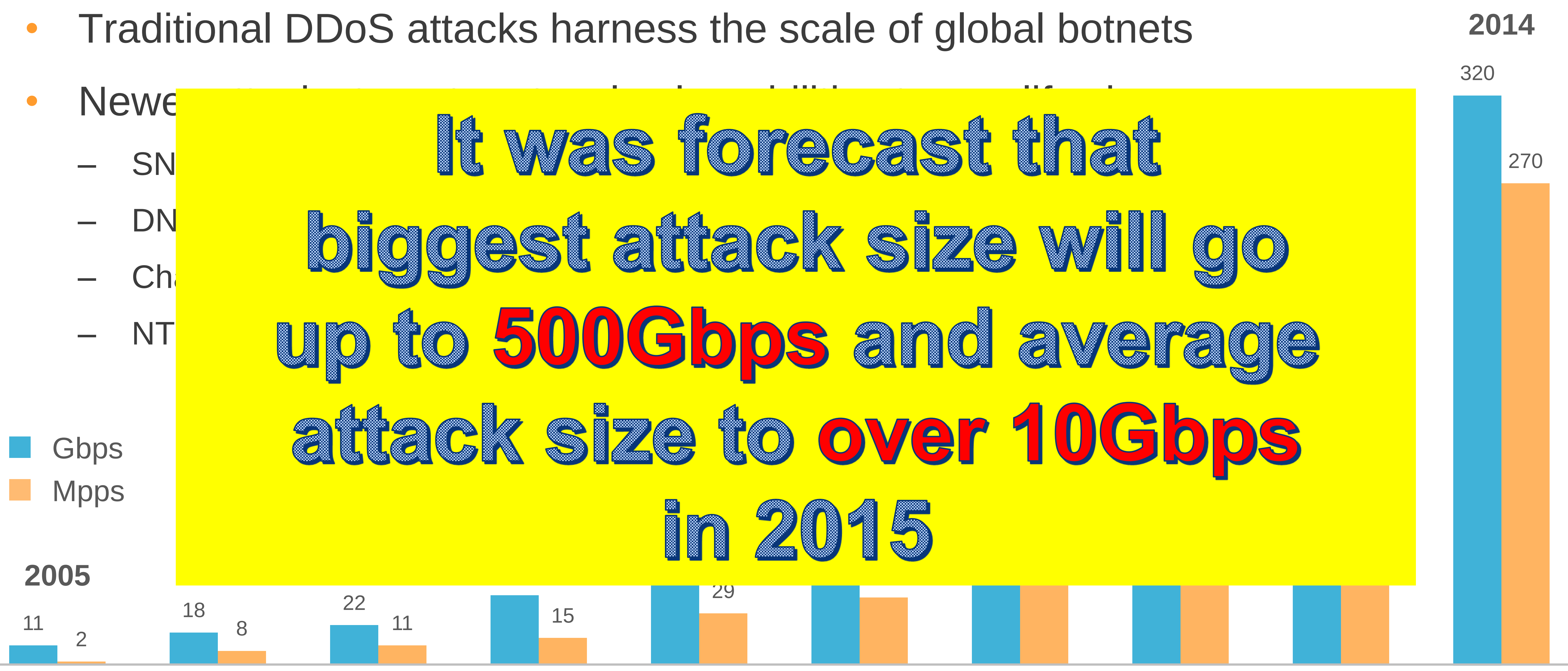
	SMEs	Large businesses
Top three threats *(Based on 'extremely concerned' responses)*	1. Cyber attack - 30% 2. Unplanned IT & telecom outages - 24% Data breach - 24% 3. Interruption to utility supply - 19%	1. Cyber attack - 47% 2. Unplanned IT & telecom outages - 37% 3. Data breach - 34%
Top three trends	1. Use of Internet for malicious attacks - 79% 2. Loss of key employee - 67% 3. Influence of social media - 58%	1. Use of Internet for malicious attacks - 82% 2. Influence of social media - 64% 3. Potential emergence of a global pandemic - 61%
Conducting Trend Analysis	59%	77%
Use of ISO 22301	50%	53%
Level Of BC Investment	Up - 20% Down - 11% Unchanged - 56%	Up - 24% Down - 12% Unchanged - 54%

--Business Continuity Institute, Horizon Scan Report 2015

Attacks Are Growing in Size

- Traditional DDoS attacks harness the scale of global botnets
- Newe
  - SN
  - DN
  - Ch
  - NT

It was forecast that biggest attack size will go up to 500Gbps and average attack size to over 10Gbps in 2015



Our digital walls are struggling

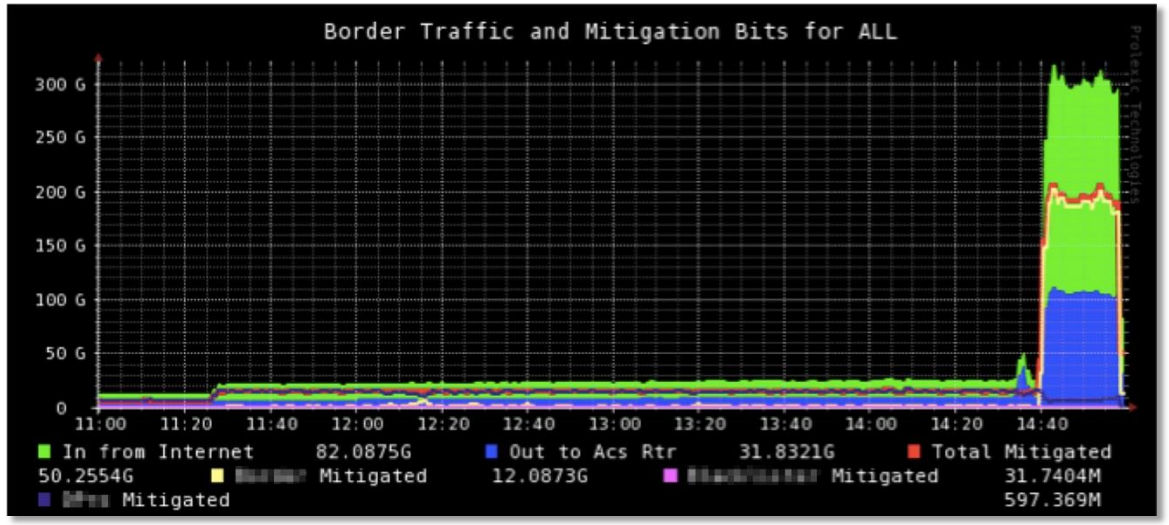
Source: World War Z movie

Web Apps DDoS - 320 Gbps attack in Asia (Q3 2014)

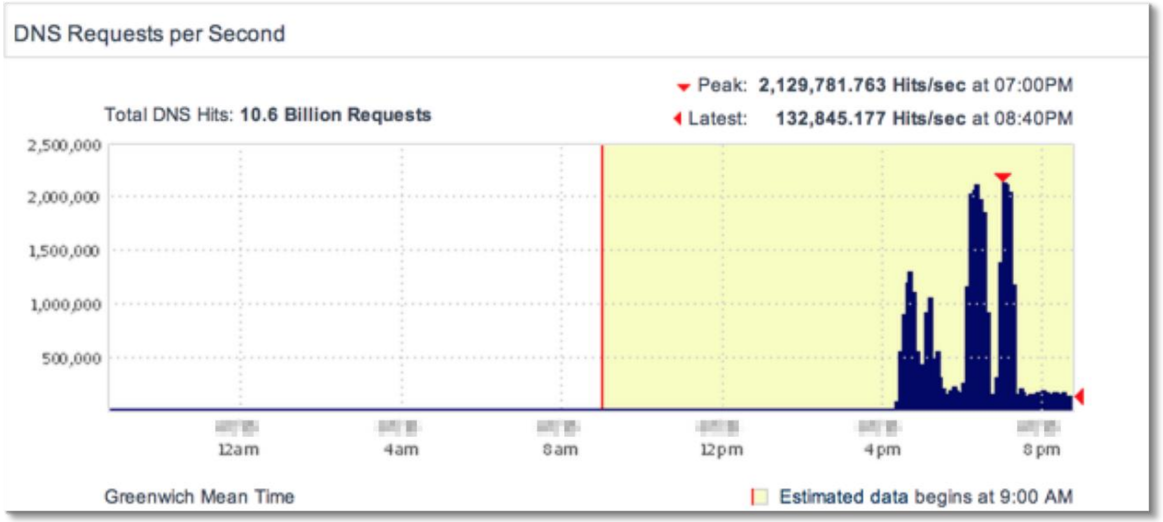
- Largest attack ever mitigated by Akamai against a single customer
- Targeted primary website, supporting network infrastructure, and DNS
- Multiple attack vectors:
  - SYN / UDP floods against an entire subnet
  - Volumetric attack against DNS
- Attack characteristics:
  - 320 Gbps and 71.5 Mpps peak DDoS attack traffic
  - 2.1 million requests/s peak DNS attack traffic

Point to ponder: 17 x 100Gbps attacks July to Sept to one single target

DDoS Attack:

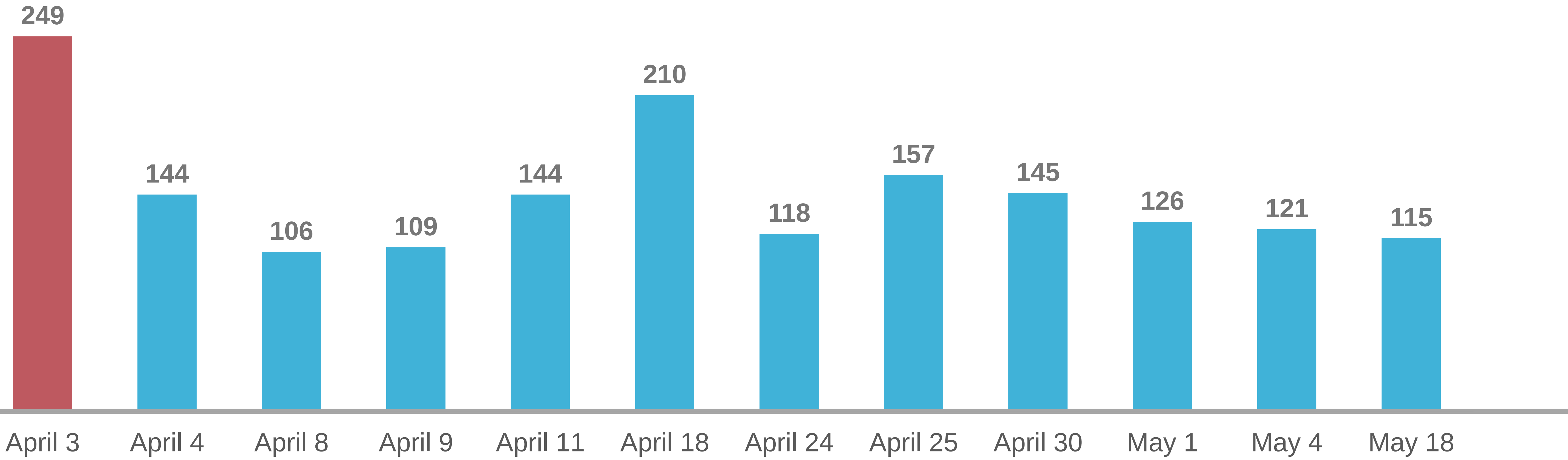


DNS Attack:



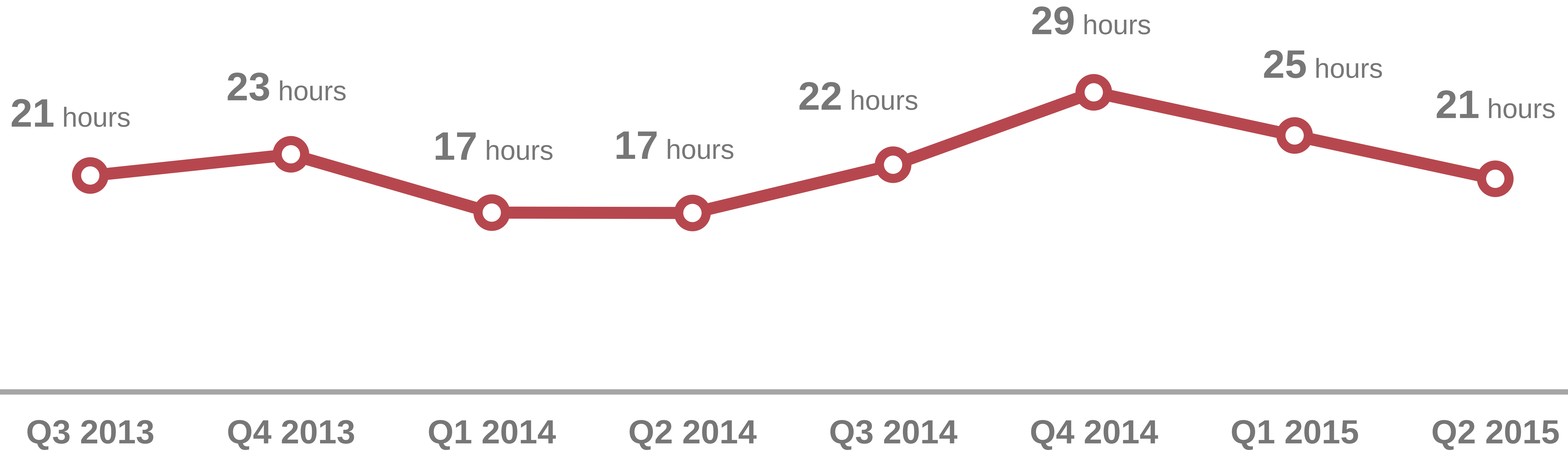
Attacks > 100 Gbps mitigated in Q2 2015

- **MEGA ATTACKS**



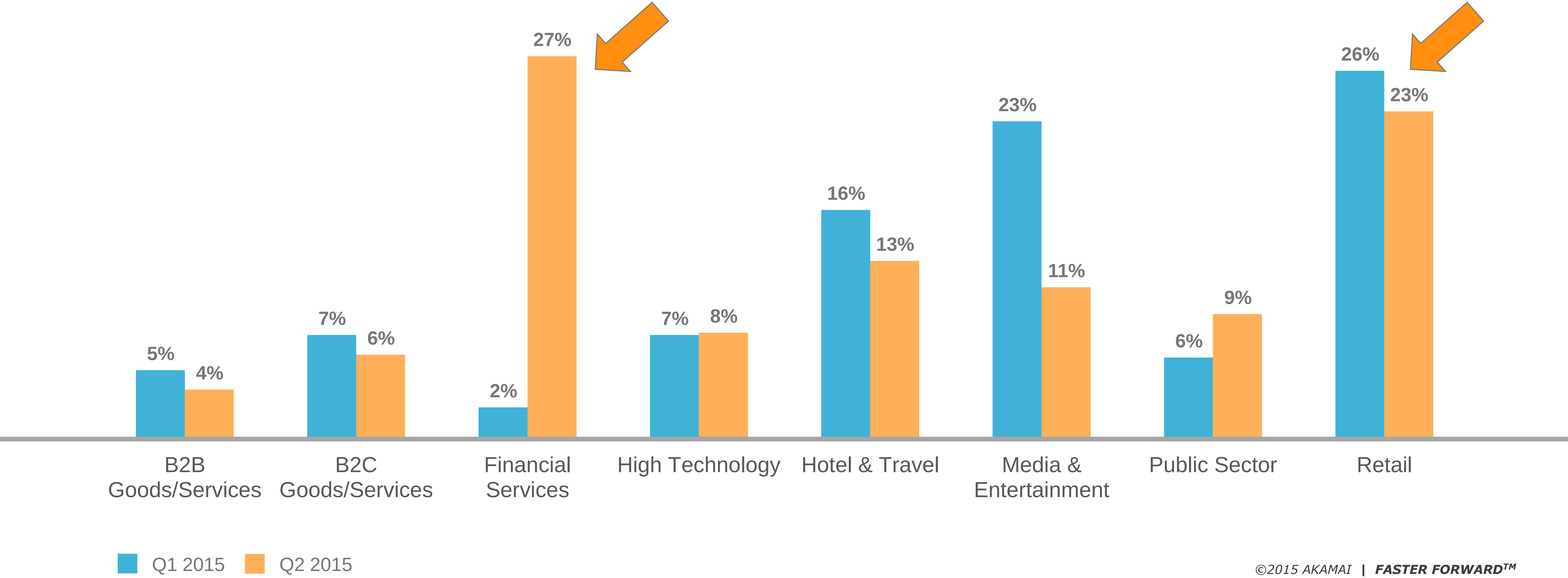
- Straining IT staff

• AVERAGE DURATION



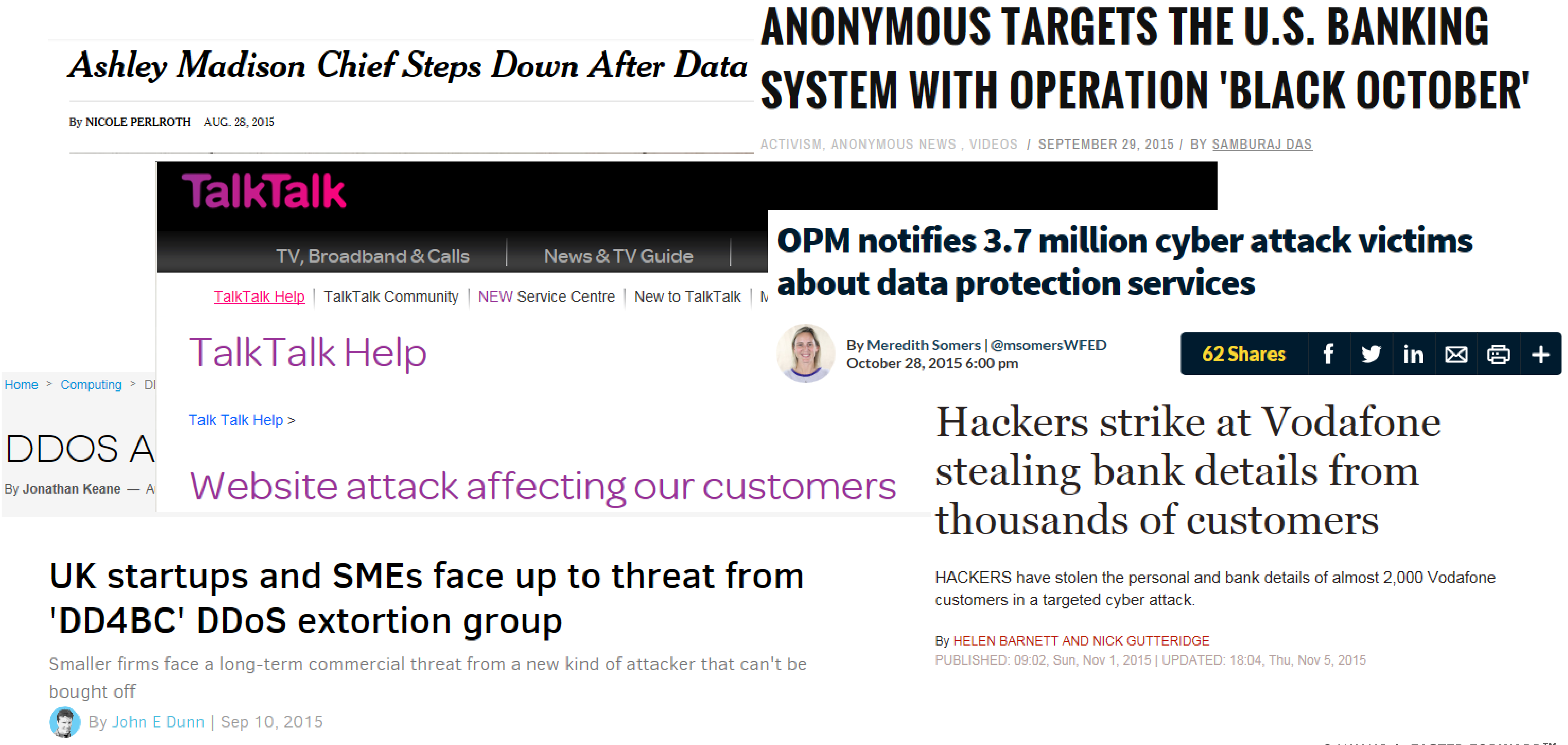
- Web attack frequency

BY TARGET INDUSTRY



	Q1 2015	Q2 2015
B2B Goods/Services	5%	4%
B2C Goods/Services	7%	6%
Financial Services	2%	27%
High Technology	7%	8%
Hotel & Travel	16%	13%
Media & Entertainment	23%	11%
Public Sector	6%	9%
Retail	26%	23%

Increasing and Devastating



ANONYMOUS TARGETS THE U.S. BANKING SYSTEM WITH OPERATION 'BLACK OCTOBER'

ACTIVISM, ANONYMOUS NEWS , VIDEOS / SEPTEMBER 29, 2015 / BY SAMBURAJ DAS

Ashley Madison Chief Steps Down After Data

By NICOLE PERLROTH AUG. 28, 2015

TalkTalk

TV, Broadband & Calls
News & TV Guide
TalkTalk Help | TalkTalk Community | NEW Service Centre | New to TalkTalk | M

TalkTalk Help

Talk Talk Help >

Website attack affecting our customers

OPM notifies 3.7 million cyber attack victims about data protection services

By Meredith Somers | @msomersWFED
October 28, 2015 6:00 pm

DDOS A

By Jonathan Keane — A

Hackers strike at Vodafone stealing bank details from thousands of customers

HACKERS have stolen the personal and bank details of almost 2,000 Vodafone customers in a targeted cyber attack.

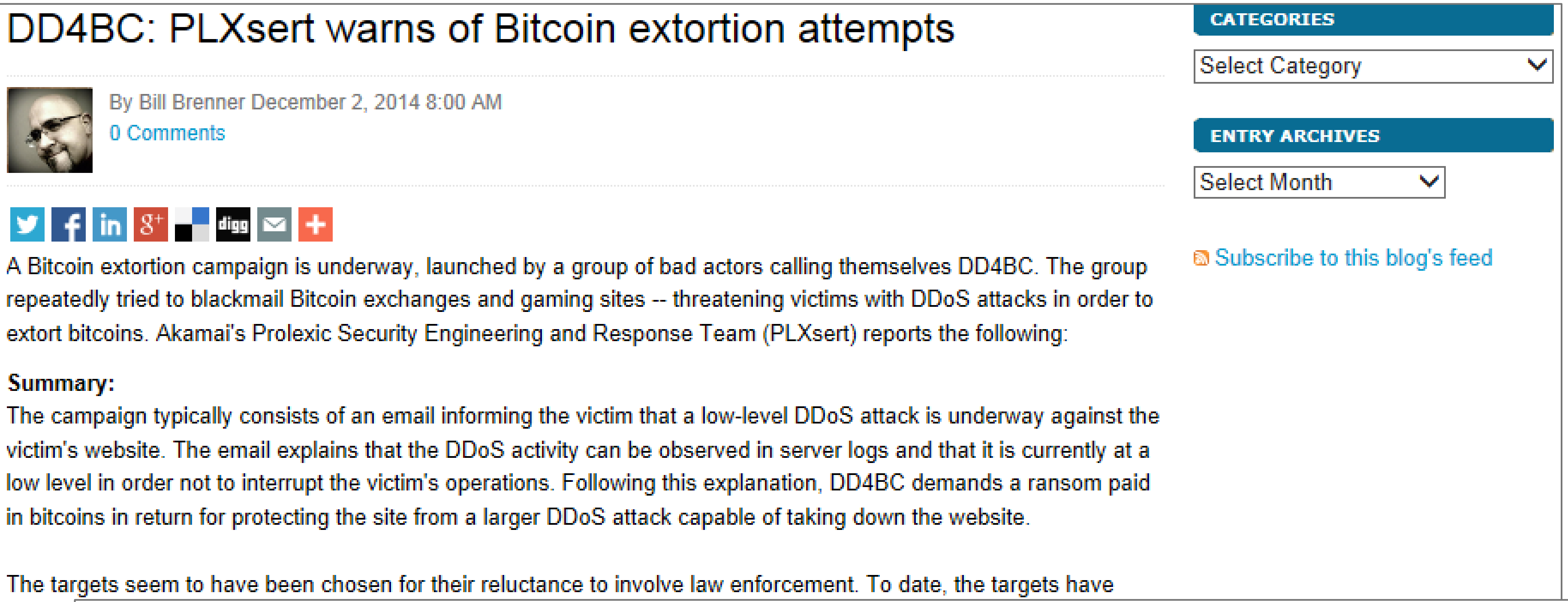
By HELEN BARNETT AND NICK GUTTERIDGE
PUBLISHED: 09:02, Sun, Nov 1, 2015 | UPDATED: 18:04, Thu, Nov 5, 2015

UK startups and SMEs face up to threat from 'DD4BC' DDoS extortion group

Smaller firms face a long-term commercial threat from a new kind of attacker that can't be bought off

By John E Dunn | Sep 10, 2015

Latest Attacks by DD4BC



DD4BC: PLXsert warns of Bitcoin extortion attempts

By Bill Brenner December 2, 2014 8:00 AM
0 Comments

A Bitcoin extortion campaign is underway, launched by a group of bad actors calling themselves DD4BC. The group repeatedly tried to blackmail Bitcoin exchanges and gaming sites -- threatening victims with DDoS attacks in order to extort bitcoins. Akamai's Prolexic Security Engineering and Response Team (PLXsert) reports the following:

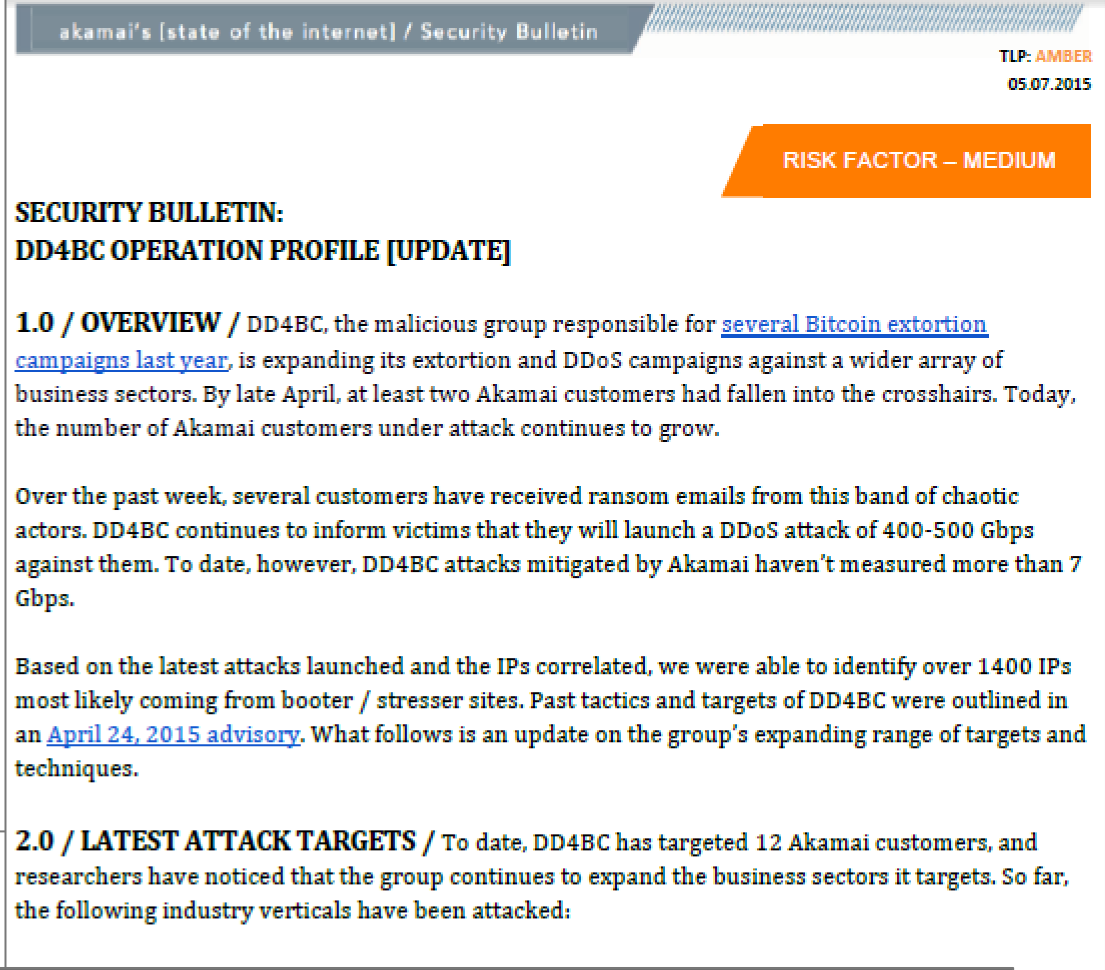
Summary:
The campaign typically consists of an email informing the victim that a low-level DDoS attack is underway against the victim's website. The email explains that the DDoS activity can be observed in server logs and that it is currently at a low level in order not to interrupt the victim's operations. Following this explanation, DD4BC demands a ransom paid in bitcoins in return for protecting the site from a larger DDoS attack capable of taking down the website.

The targets seem to have been chosen for their reluctance to involve law enforcement. To date, the targets have been a
bitcoin
scrutin

This m
paid by
major c

PLXse
payloa
have a

Curren
operati
payme



SECURITY BULLETIN:
DD4BC OPERATION PROFILE [UPDATE]

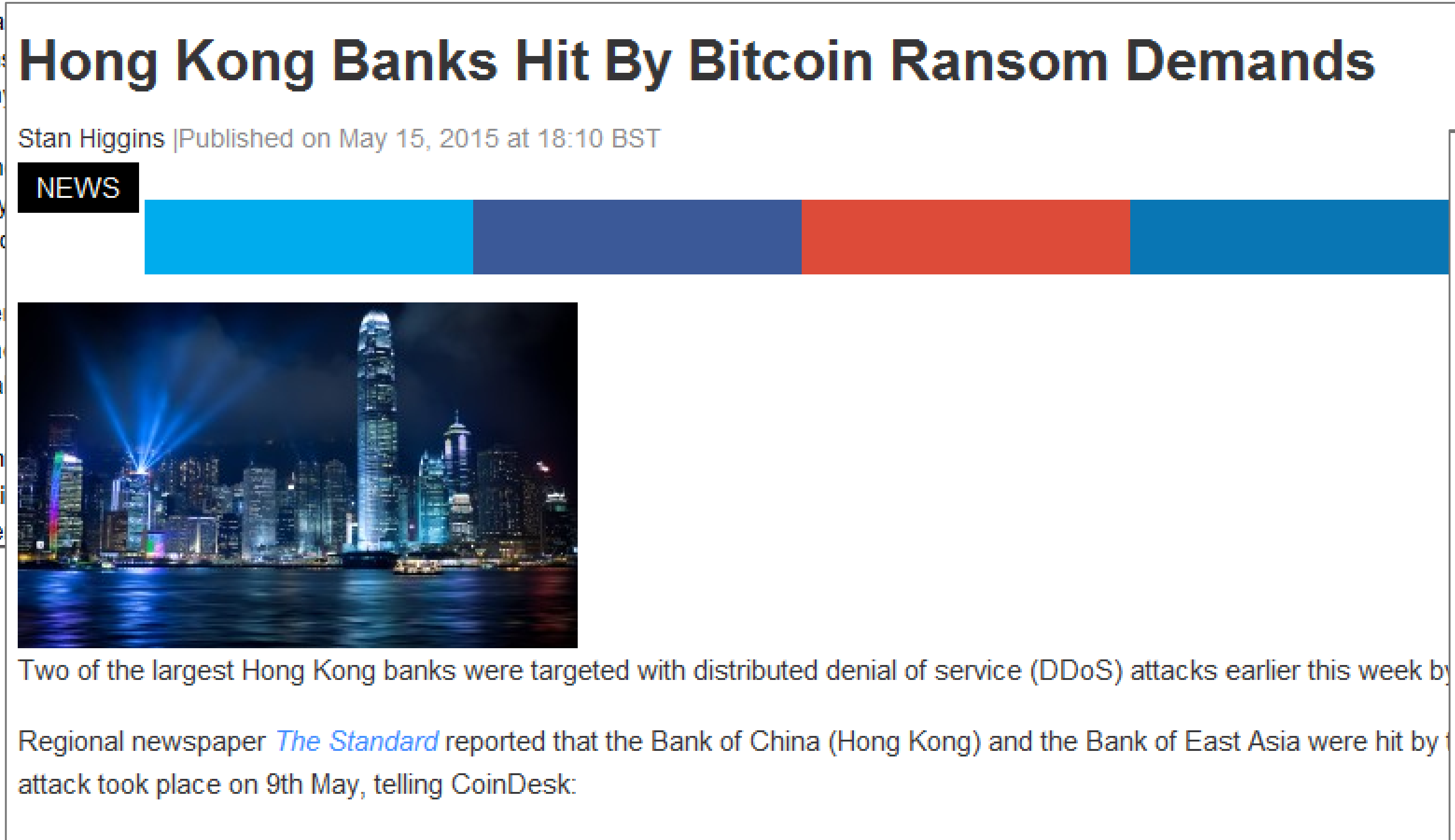
1.0 / OVERVIEW / DD4BC, the malicious group responsible for several Bitcoin extortion campaigns last year, is expanding its extortion and DDoS campaigns against a wider array of business sectors. By late April, at least two Akamai customers had fallen into the crosshairs. Today, the number of Akamai customers under attack continues to grow.

Over the past week, several customers have received ransom emails from this band of chaotic actors. DD4BC continues to inform victims that they will launch a DDoS attack of 400-500 Gbps against them. To date, however, DD4BC attacks mitigated by Akamai haven't measured more than 7 Gbps.

Based on the latest attacks launched and the IPs correlated, we were able to identify over 1400 IPs most likely coming from booter / stresser sites. Past tactics and targets of DD4BC were outlined in an April 24, 2015 advisory. What follows is an update on the group's expanding range of targets and techniques.

2.0 / LATEST ATTACK TARGETS / To date, DD4BC has targeted 12 Akamai customers, and researchers have noticed that the group continues to expand the business sectors it targets. So far, the following industry verticals have been attacked:

ived



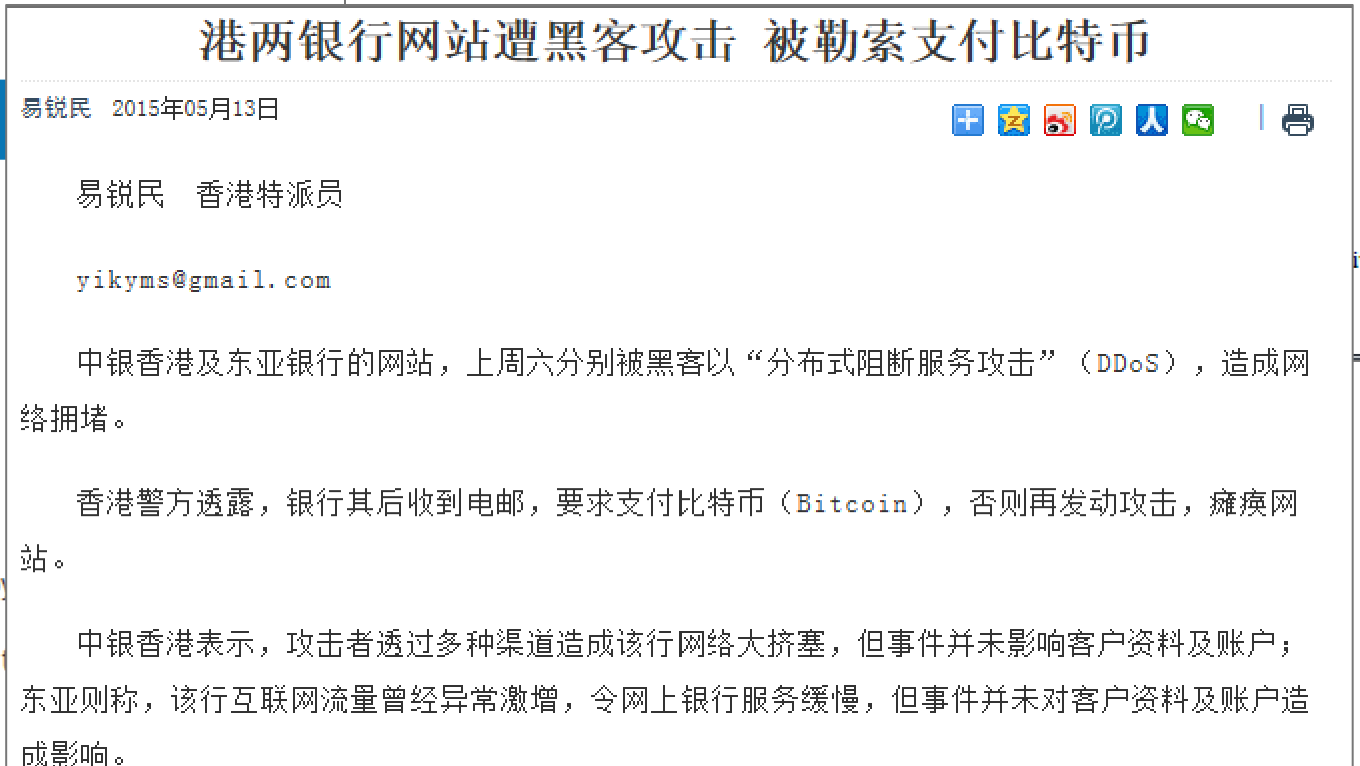
Hong Kong Banks Hit By Bitcoin Ransom Demands

Stan Higgins |Published on May 15, 2015 at 18:10 BST

NEWS

Two of the largest Hong Kong banks were targeted with distributed denial of service (DDoS) attacks earlier this week by

Regional newspaper *The Standard* reported that the Bank of China (Hong Kong) and the Bank of East Asia were hit by attack took place on 9th May, telling CoinDesk:



港两银行网站遭黑客攻击 被勒索支付比特币

易锐民　2015年05月13日

易锐民　香港特派员

yikyms@gmail.com

中银香港及东亚银行的网站，上周六分别被黑客以“分布式阻断服务攻击”（DDoS），造成网络拥堵。

香港警方透露，银行其后收到电邮，要求支付比特币（Bitcoin），否则再发动攻击，瘫痪网站。

中银香港表示，攻击者透过多种渠道造成该行网络大挤塞，但事件并未影响客户资料及账户；东亚则称，该行互联网流量曾经异常激增，令网上银行服务缓慢，但事件并未对客户资料及账户造成影响。

Change of Attack Objectives

- Retaliation
- Competition
- “Justice”
- Firepower Test
- Reputation
- Nation-to-Nation
- Public Movement

- Extortion
- DDoS-for-hire
- Ransom

Akamai Security Bulletin on DD4BC

Latest Update:

To date,DD4BC has targeted 114 Akamai customers. Industry verticals have been attacked incl.:

● Payment Processing
● Banking & Credit Unions
● Gambling
● Oil & gas
● E-Commerce
● Betting Agencies
● High Tech Consulting/Services

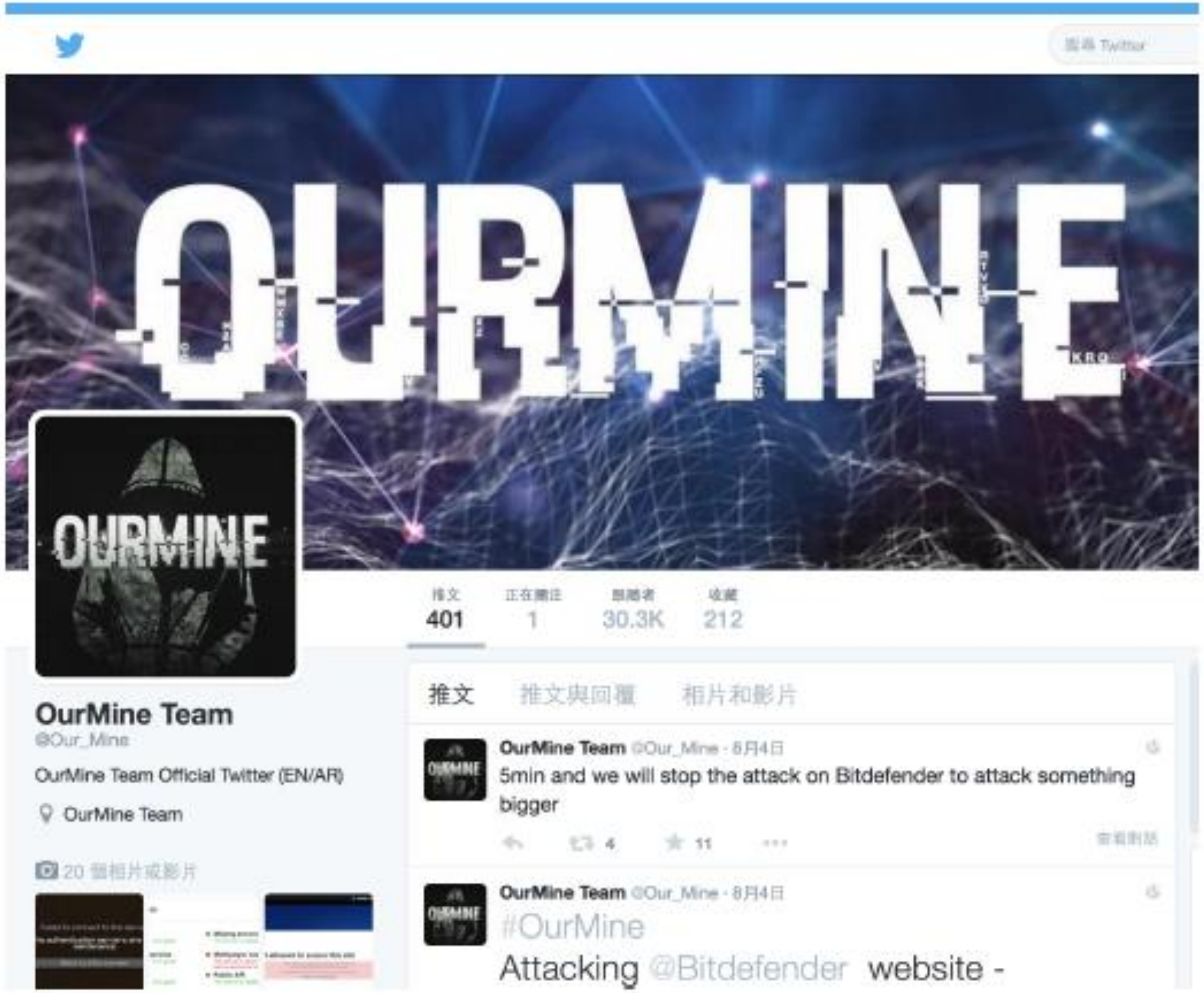
AttackTypes:

SYN Flood, UDP Fragment Flood, CharGEN Flood, *GET Flood*, NTP reflection flood, CharGEN reflection flood, SSDP reflection flood. **Campaign has peak attack traffic over 15Gbps**

Conclusion:

- Expect the group to continue expanding its targeting to other verticals susceptible of financial loss due to downtime.
- Similar to an “express kidnapping” – small ransoms
- Likely already received payments from the threats made to some of these victims
- Activity will increase as copycats enter the game
- Previously targeted victims likely only have the choice of either paying malicious actors or seeking DDoS protection services

New kid on the street



OurMine Team
@Our_Mine
OurMine Team Official Twitter (EN/AR)
OurMine Team

OurMine Team @Our_Mine · 8月4日
5min and we will stop the attack on Bitdefender to attack something bigger

OurMine Team @Our_Mine · 8月4日
#OurMine
Attacking @Bitdefender website -

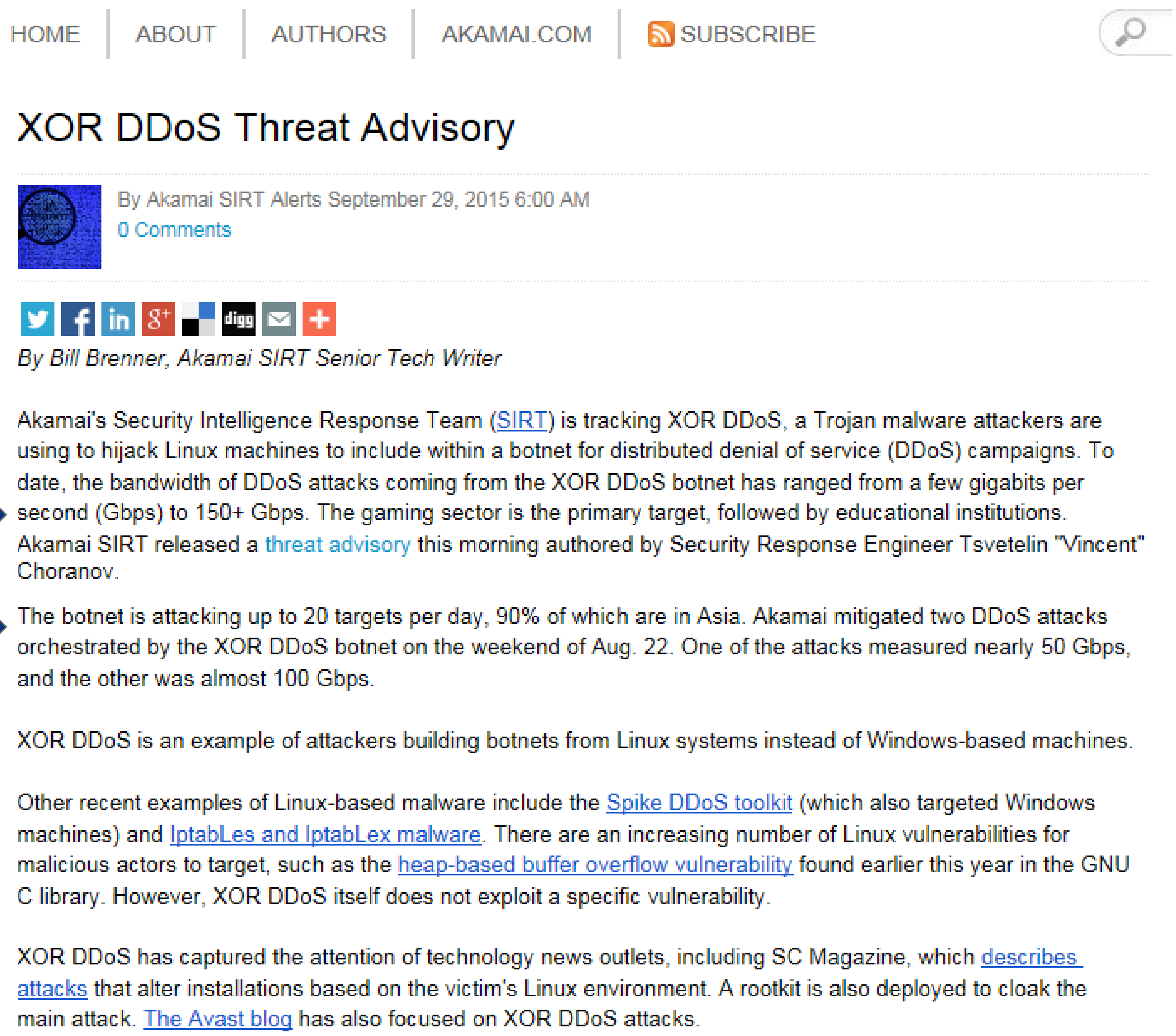
DDoS attacks across the financial sector

No outages have been reported

The largest attack peaked at 117 Gbps

Not announce target lists in advance

XOR DDoS



XOR DDoS Threat Advisory

By Akamai SIRT Alerts September 29, 2015 6:00 AM
0 Comments

By Bill Brenner, Akamai SIRT Senior Tech Writer

Akamai's Security Intelligence Response Team (SIRT) is tracking XOR DDoS, a Trojan malware attackers are using to hijack Linux machines to include within a botnet for distributed denial of service (DDoS) campaigns. To date, the bandwidth of DDoS attacks coming from the XOR DDoS botnet has ranged from a few gigabits per second (Gbps) to 150+ Gbps. The gaming sector is the primary target, followed by educational institutions. Akamai SIRT released a threat advisory this morning authored by Security Response Engineer Tsvetelin "Vincent" Choranov.

The botnet is attacking up to 20 targets per day, 90% of which are in Asia. Akamai mitigated two DDoS attacks orchestrated by the XOR DDoS botnet on the weekend of Aug. 22. One of the attacks measured nearly 50 Gbps, and the other was almost 100 Gbps.

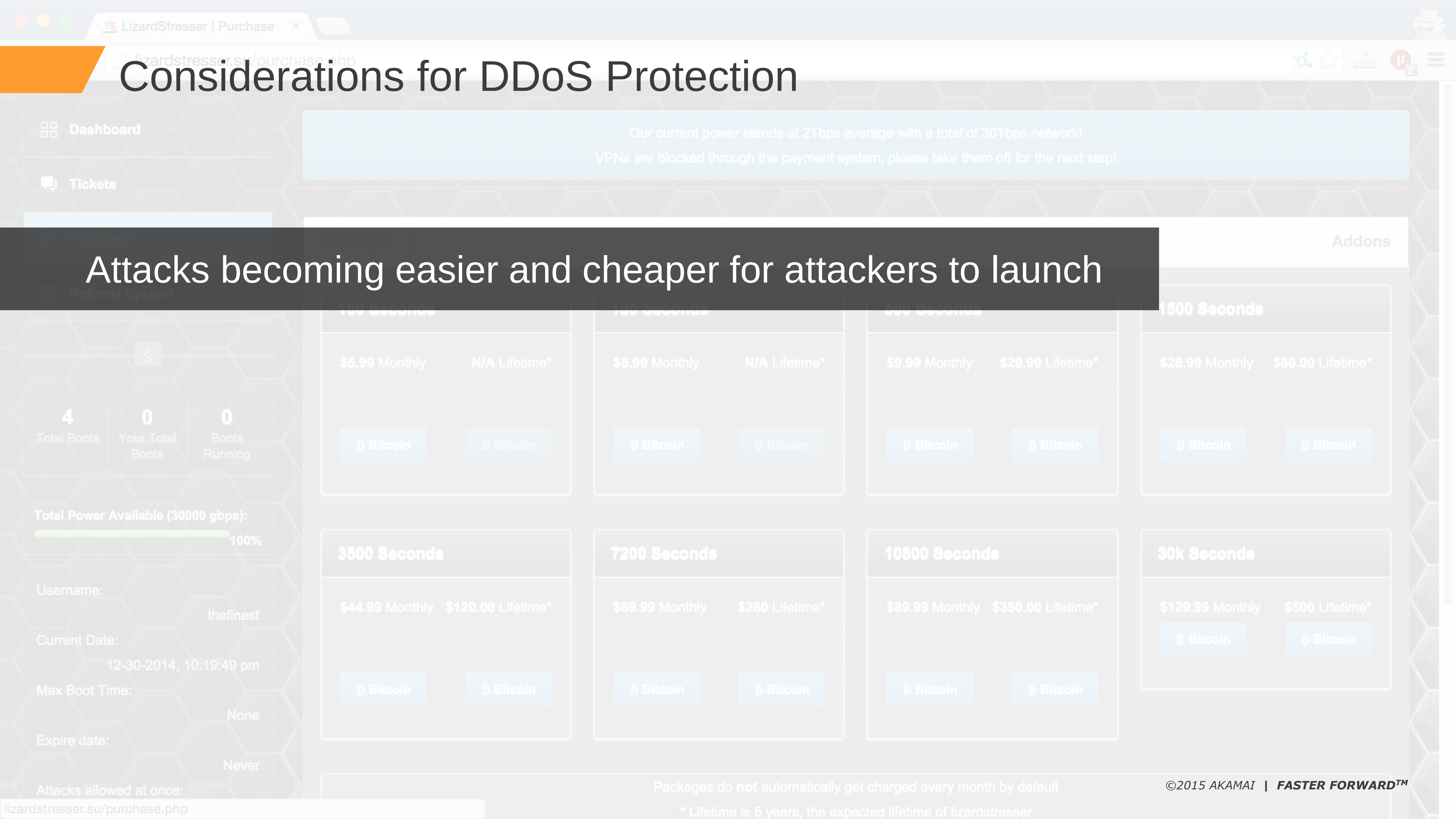
XOR DDoS is an example of attackers building botnets from Linux systems instead of Windows-based machines.

Other recent examples of Linux-based malware include the Spike DDoS toolkit (which also targeted Windows machines) and IptabLes and IptabLex malware. There are an increasing number of Linux vulnerabilities for malicious actors to target, such as the heap-based buffer overflow vulnerability found earlier this year in the GNU C library. However, XOR DDoS itself does not exploit a specific vulnerability.

XOR DDoS has captured the attention of technology news outlets, including SC Magazine, which describes attacks that alter installations based on the victim's Linux environment. A rootkit is also deployed to cloak the main attack. The Avast blog has also focused on XOR DDoS attacks.

Considerations for DDoS Protection

Attacks becoming easier and cheaper for attackers to launch



LizardStresser | Purchase

lizardstresser.su/purchase.php

Dashboard

Tickets

Purchase

Referral System

4 Total Boots | 0 Your Total Boots | 0 Boots Running

Total Power Available (30000 gbps): 100%

Username: thefinest

Current Date: 12-30-2014, 10:19:49 pm

Max Boot Time: None

Expire date: Never

Attacks allowed at once:

Our current power stands at 2Tbps average with a total of 30Tbps network!

VPNs are blocked through the payment system, please take them off for the next step!

Packages

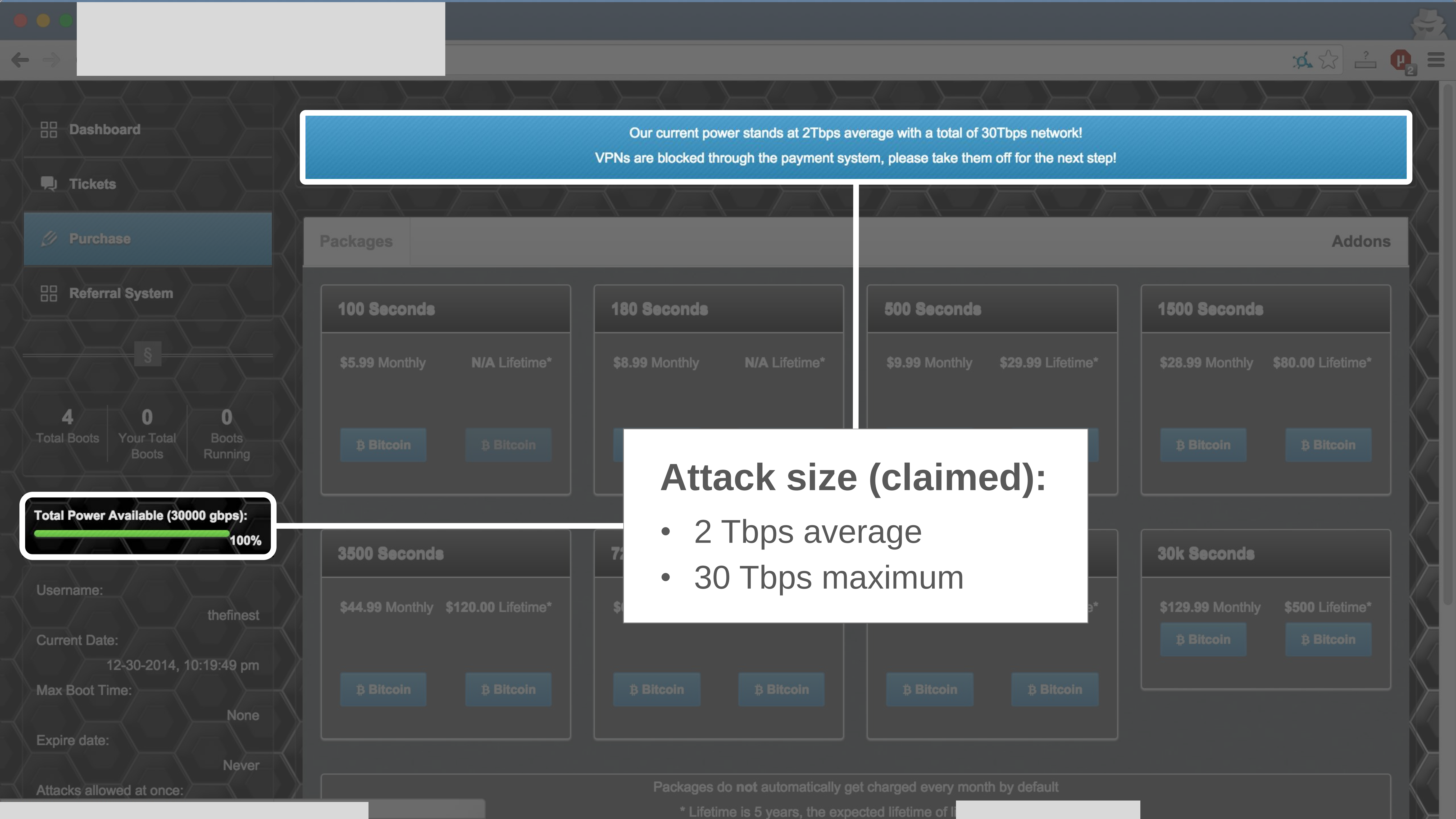
Addons

Package	Monthly	Lifetime
100 Seconds	$5.99 Monthly ₿ Bitcoin	N/A Lifetime* ₿ Bitcoin
180 Seconds	$8.99 Monthly ₿ Bitcoin	N/A Lifetime* ₿ Bitcoin
300 Seconds	$9.99 Monthly ₿ Bitcoin	$29.99 Lifetime* ₿ Bitcoin
1500 Seconds	$28.99 Monthly ₿ Bitcoin	$80.00 Lifetime* ₿ Bitcoin
3500 Seconds	$44.99 Monthly ₿ Bitcoin	$120.00 Lifetime* ₿ Bitcoin
7200 Seconds	$69.99 Monthly ₿ Bitcoin	$280 Lifetime* ₿ Bitcoin
10800 Seconds	$89.99 Monthly ₿ Bitcoin	$350.00 Lifetime* ₿ Bitcoin
30k Seconds	$129.99 Monthly ₿ Bitcoin	$500 Lifetime* ₿ Bitcoin

Packages do not automatically get charged every month by default

* Lifetime is 5 years, the expected lifetime of lizardstresser

lizardstresser.su/purchase.php



[redacted]

Our current power stands at 2Tbps average with a total of 30Tbps network!
VPNs are blocked through the payment system, please take them off for the next step!

4	0	0
Total Boots	Your Total Boots	Boots Running

Total Power Available (30000 gbps): 100%

Username: thefinest

Current Date: 12-30-2014, 10:19:49 pm

Max Boot Time: None

Expire date: Never

Attacks allowed at once:

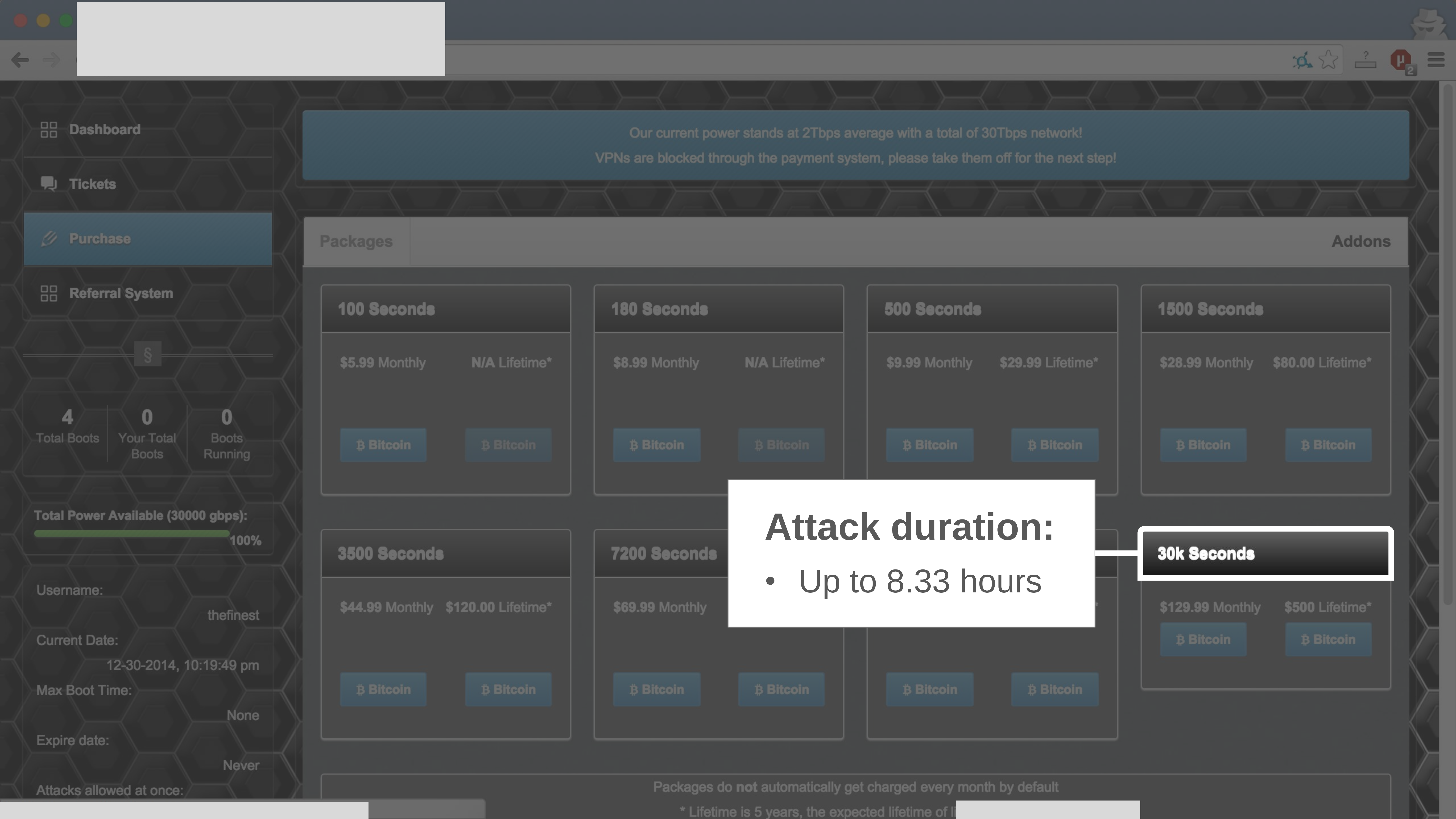
Package	Monthly	Lifetime*
100 Seconds	$5.99 Monthly	N/A Lifetime*
180 Seconds	$8.99 Monthly	N/A Lifetime*
500 Seconds	$9.99 Monthly	$29.99 Lifetime*
1500 Seconds	$28.99 Monthly	$80.00 Lifetime*
3500 Seconds	$44.99 Monthly	$120.00 Lifetime*
30k Seconds	$129.99 Monthly	$500 Lifetime*

Packages do **not** automatically get charged every month by default

* Lifetime is 5 years, the expected lifetime of l [redacted]

Attack size (claimed):

- 2 Tbps average
- 30 Tbps maximum



[redacted]

Dashboard

Tickets

Purchase

Referral System

§

4 Total Boots | 0 Your Total Boots | 0 Boots Running

Total Power Available (30000 gbps): 100%

Username: thefinest

Current Date: 12-30-2014, 10:19:49 pm

Max Boot Time: None

Expire date: Never

Attacks allowed at once:

[redacted]

Our current power stands at 2Tbps average with a total of 30Tbps network!

VPNs are blocked through the payment system, please take them off for the next step!

Packages | Addons

100 Seconds

$5.99 Monthly | N/A Lifetime*

฿ Bitcoin | ฿ Bitcoin

180 Seconds

$8.99 Monthly | N/A Lifetime*

฿ Bitcoin | ฿ Bitcoin

500 Seconds

$9.99 Monthly | $29.99 Lifetime*

฿ Bitcoin | ฿ Bitcoin

1500 Seconds

$28.99 Monthly | $80.00 Lifetime*

฿ Bitcoin | ฿ Bitcoin

3500 Seconds

$44.99 Monthly | $120.00 Lifetime*

฿ Bitcoin | ฿ Bitcoin

7200 Seconds

$69.99 Monthly

฿ Bitcoin | ฿ Bitcoin

฿ Bitcoin | ฿ Bitcoin

30k Seconds

$129.99 Monthly | $500 Lifetime*

฿ Bitcoin | ฿ Bitcoin

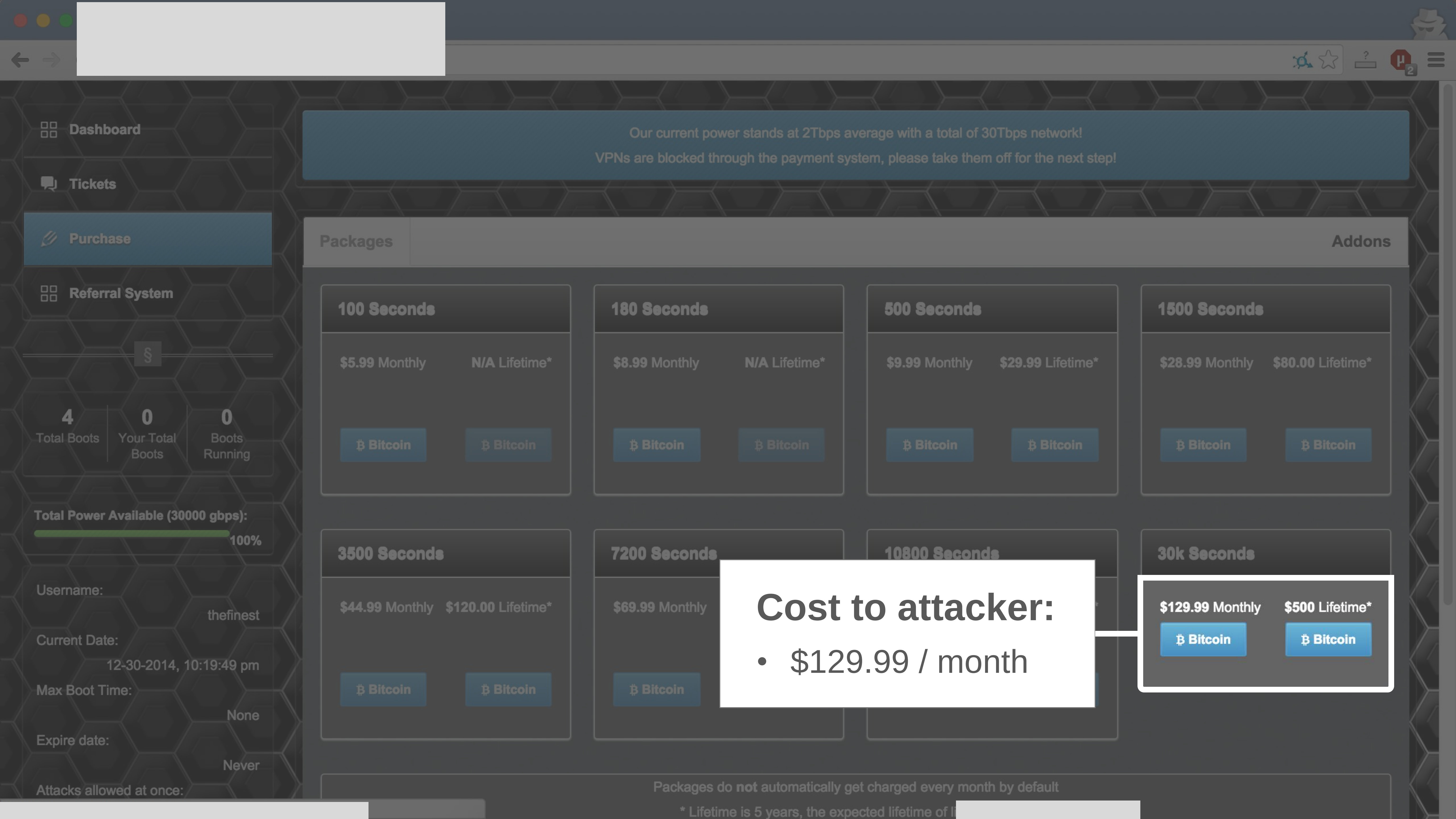
Packages do **not** automatically get charged every month by default

* Lifetime is 5 years, the expected lifetime of l

[redacted]

Attack duration:

- Up to 8.33 hours



[redacted]

4 Total Boots | 0 Your Total Boots | 0 Boots Running

Total Power Available (30000 gbps): 100%

Username: thefinest

Current Date: 12-30-2014, 10:19:49 pm

Max Boot Time: None

Expire date: Never

Attacks allowed at once:

[redacted]

Our current power stands at 2Tbps average with a total of 30Tbps network!

VPNs are blocked through the payment system, please take them off for the next step!

Package	Monthly	Lifetime
100 Seconds	$5.99 Monthly	N/A Lifetime*
180 Seconds	$8.99 Monthly	N/A Lifetime*
500 Seconds	$9.99 Monthly	$29.99 Lifetime*
1500 Seconds	$28.99 Monthly	$80.00 Lifetime*
3500 Seconds	$44.99 Monthly	$120.00 Lifetime*
7200 Seconds	$69.99 Monthly	
10800 Seconds		
30k Seconds	$129.99 Monthly	$500 Lifetime*

Packages do **not** automatically get charged every month by default

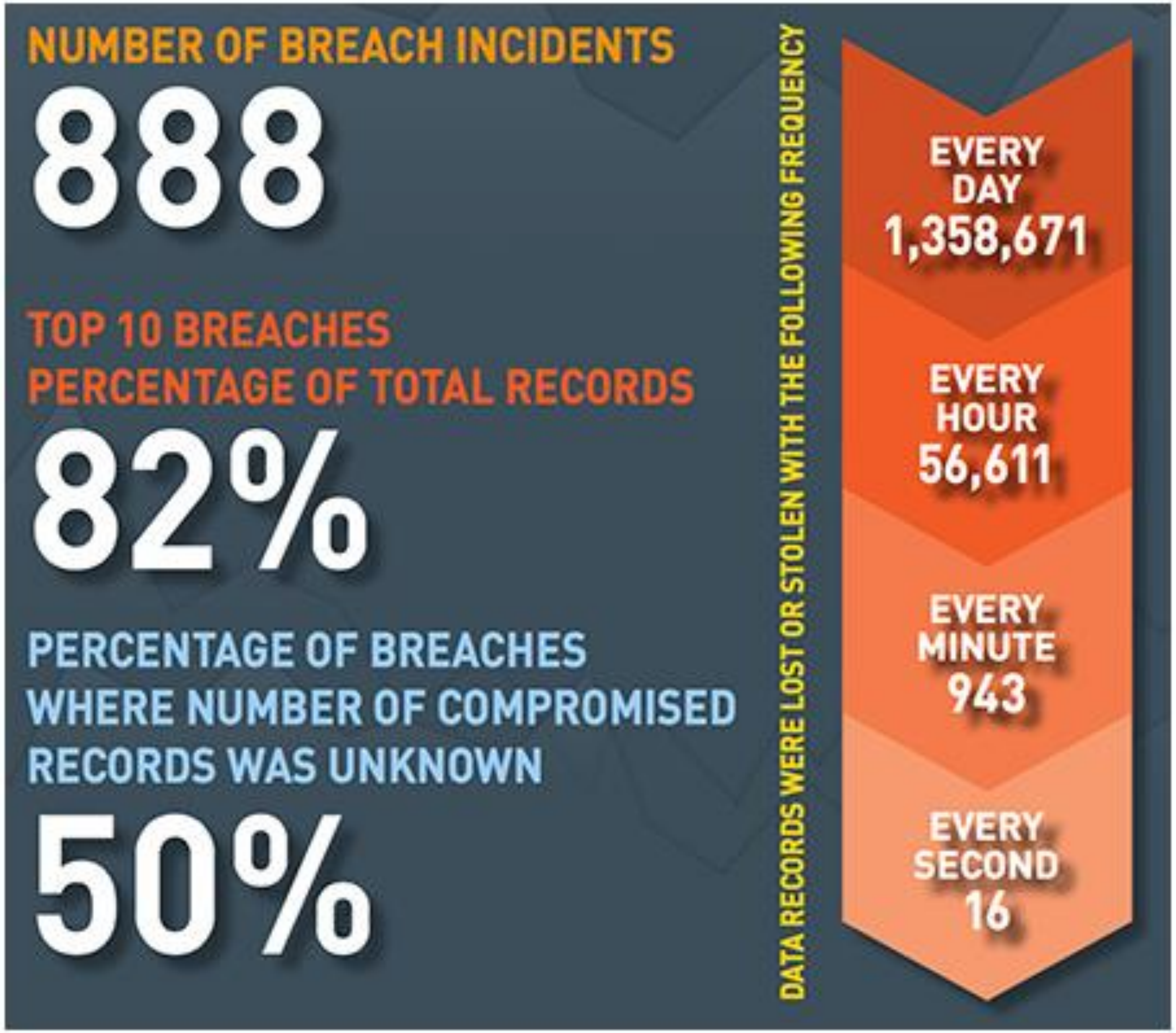
* Lifetime is 5 years, the expected lifetime of li

[redacted]

Cost to attacker:

- $129.99 / month

In the first 6 months of 2015 saw 888 data breaches, 246 million records compromised worldwide



NUMBER OF BREACH INCIDENTS

888

TOP 10 BREACHES PERCENTAGE OF TOTAL RECORDS

82%

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

50%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY 1,358,671

EVERY HOUR 56,611

EVERY MINUTE 943

EVERY SECOND 16

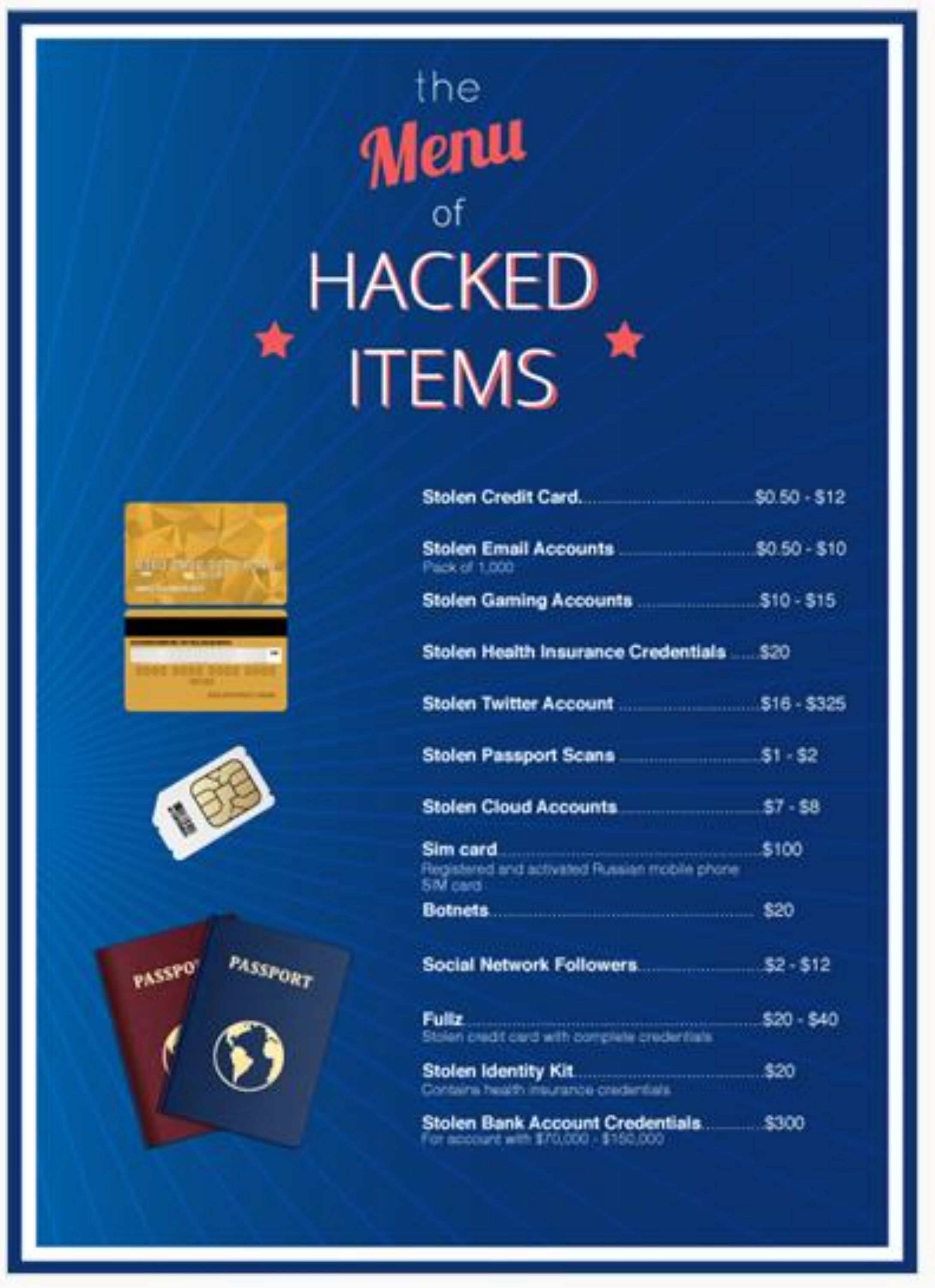
The largest breach in the first half of 2015 includes:

1) 78.8 million records exposed by identity theft attack on Anthem Insurance
2) 50-million-record breach at Turkey’s General Directorate of Population and Citizenship Affairs
3) 21-million-record breach at the U.S. Office of Personnel Management
4) 20-million-record breach at Russia’s Topface

<u>The top 10 breaches accounted for 81.4% of all compromised records</u>

Source: Gemalto

Business of Fraud



the **Menu** of HACKED ITEMS

Stolen Credit Card	$0.50 - $12
Stolen Email Accounts Pack of 1,000	$0.50 - $10
Stolen Gaming Accounts	$10 - $15
Stolen Health Insurance Credentials	$20
Stolen Twitter Account	$16 - $325
Stolen Passport Scans	$1 - $2
Stolen Cloud Accounts	$7 - $8
Sim card Registered and activated Russian mobile phone SIM card	$100
Botnets	$20
Social Network Followers	$2 - $12
Fullz Stolen credit card with complete credentials	$20 - $40
Stolen Identity Kit Contains health insurance credentials	$20
Stolen Bank Account Credentials For account with $70,000 - $150,000	$300

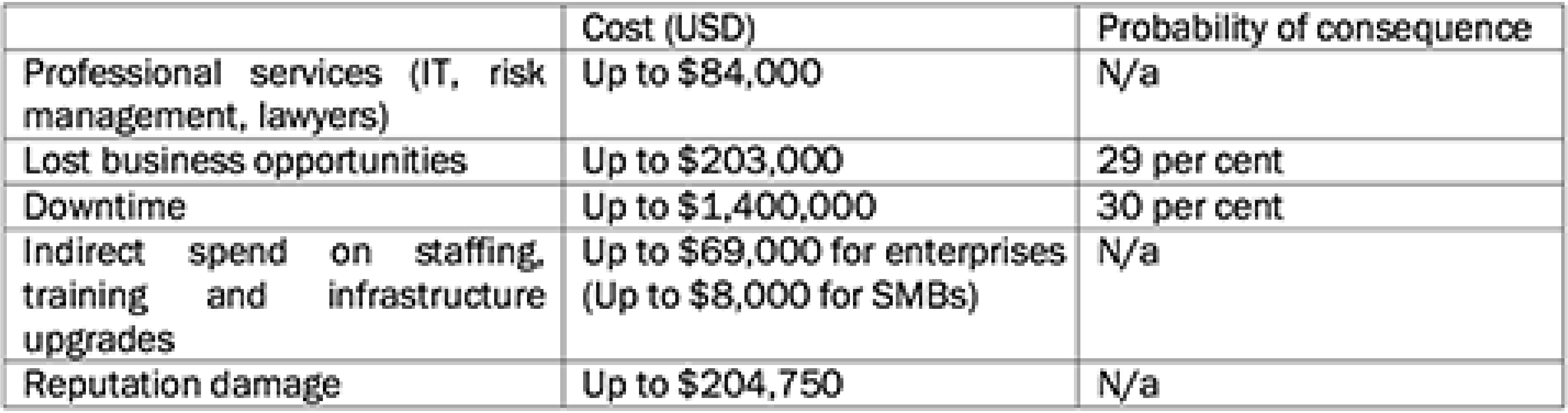
Money, Money, Money

The average budget required to recover from a security breach

= USD$551,000 for enterprises

= USD$38,000 for small and medium businesses(SMB)

The average enterprise bill and probability of some of the consequences break down as follows:



	Cost (USD)	Probability of consequence
Professional services (IT, risk management, lawyers)	Up to $84,000	N/a
Lost business opportunities	Up to $203,000	29 per cent
Downtime	Up to $1,400,000	30 per cent
Indirect spend on staffing, training and infrastructure upgrades	Up to $69,000 for enterprises (Up to $8,000 for SMBs)	N/a
Reputation damage	Up to $204,750	N/a

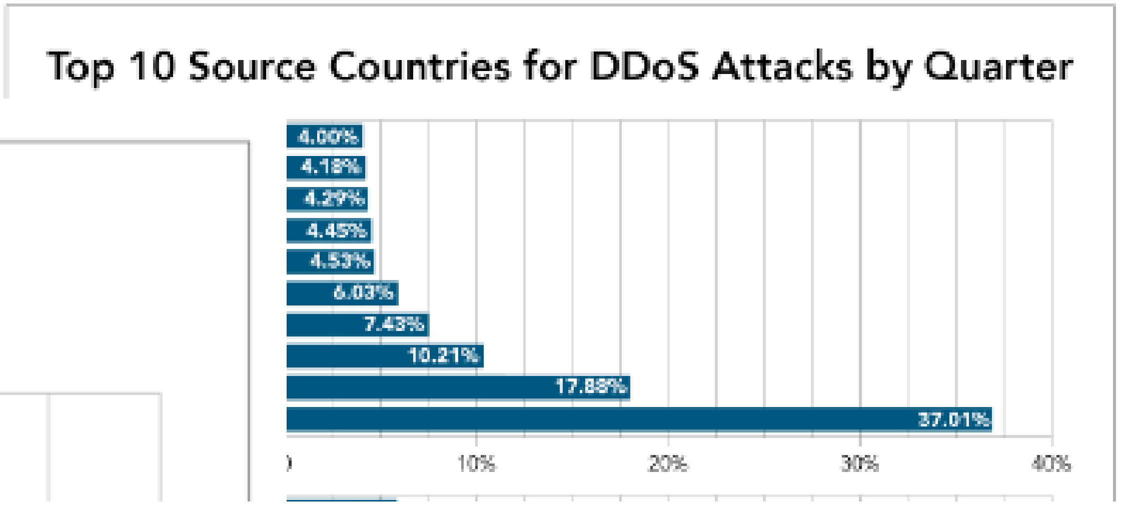
By comparison, SMBs tend to lose a significant amount of money on almost all types of breach, paying a similar high price on recovering from acts of espionage as well as DDoS and phishing attacks.

Source: worldwide survey of 5,500 companies conducted by Kaspersky Lab in cooperation with B2B International

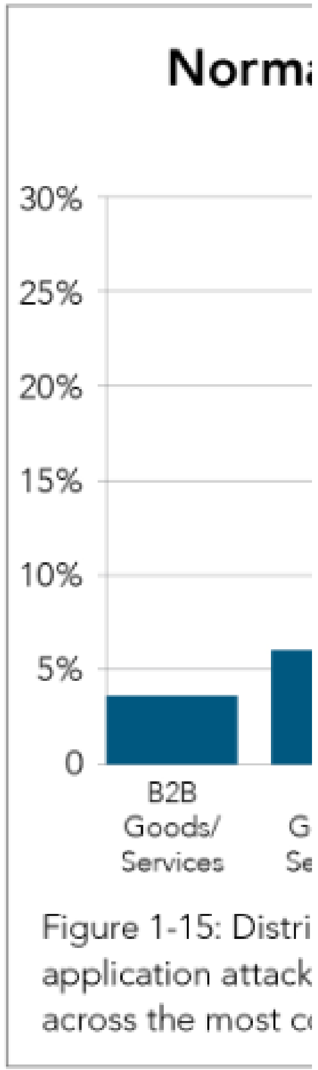
Q2 2015 State of the Internet Security Report

Top 10 Source Countries for Web Application Attacks, Q2 2015

ency by Industry

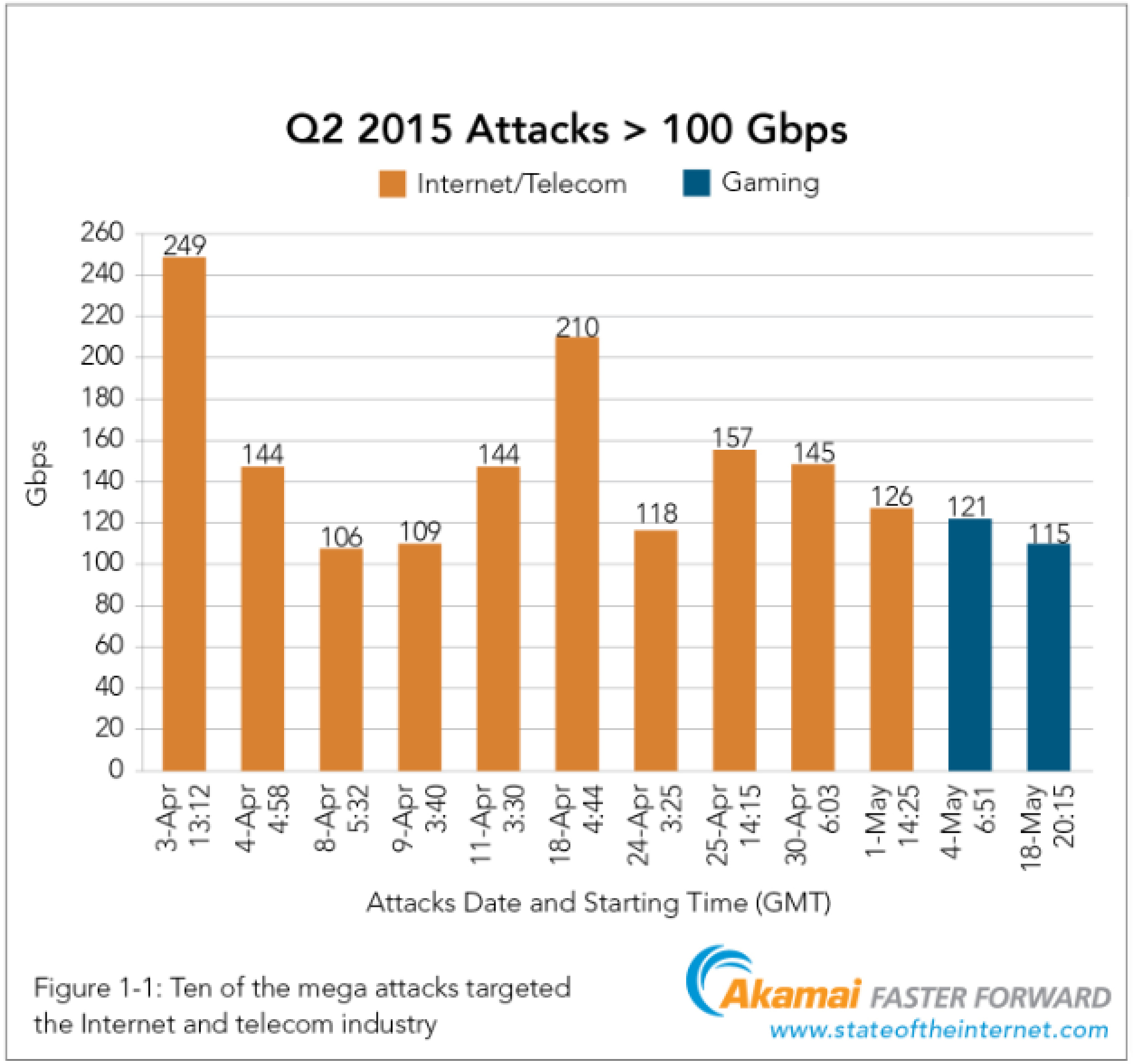


Top 10 Source Countries for DDoS Attacks by Quarter



Norm

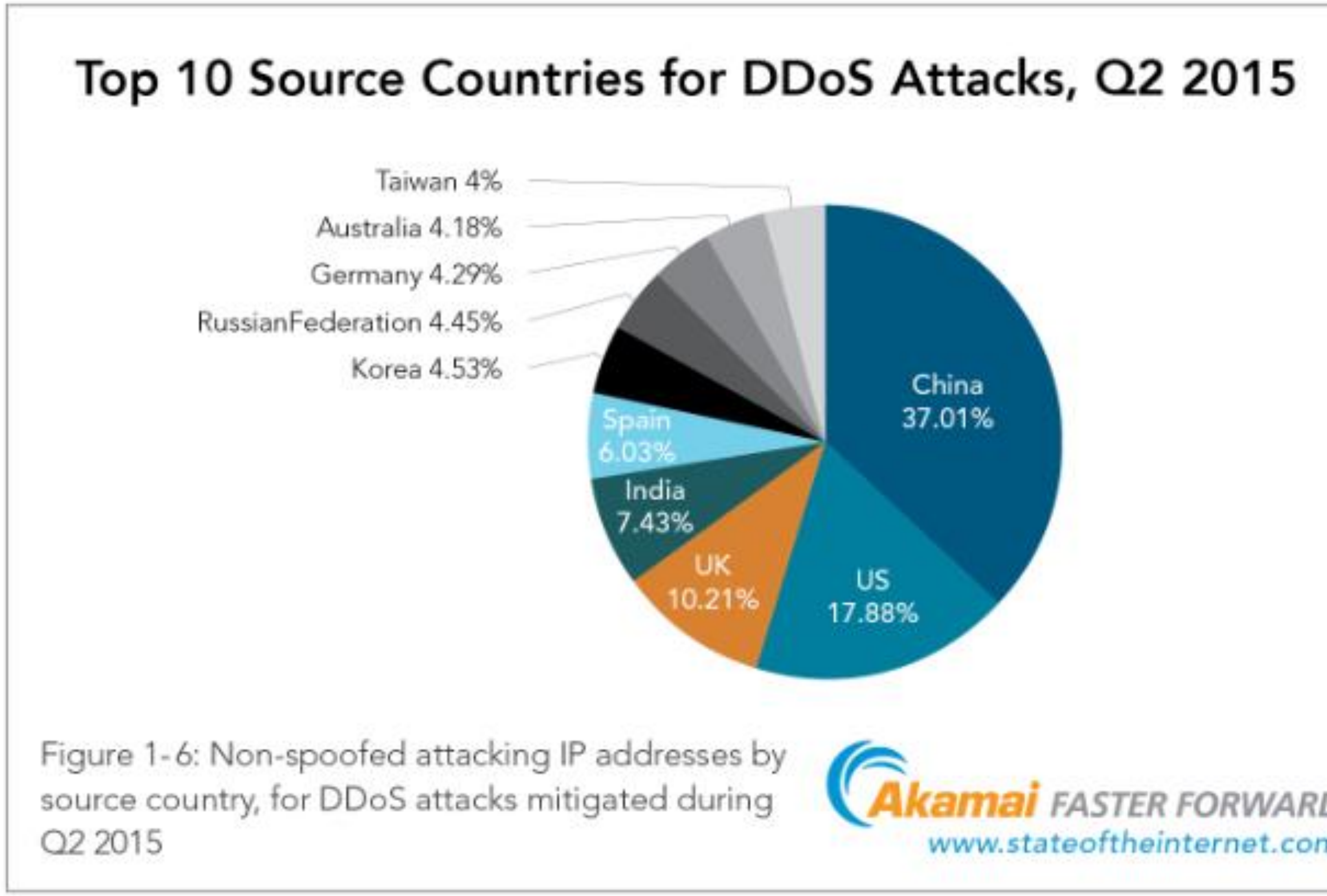
Figure 1-15: Distri application attack across the most c



Q2 2015 Attacks > 100 Gbps

Figure 1-1: Ten of the mega attacks targeted the Internet and telecom industry

Akamai FASTER FORWARD www.stateoftheinternet.com



Top 10 Source Countries for DDoS Attacks, Q2 2015

Figure 1-6: Non-spoofed attacking IP addresses by source country, for DDoS attacks mitigated during Q2 2015

Akamai FASTER FORWARD www.stateoftheinternet.com

2015: How Companies Now Prepare For Cyber Attacks

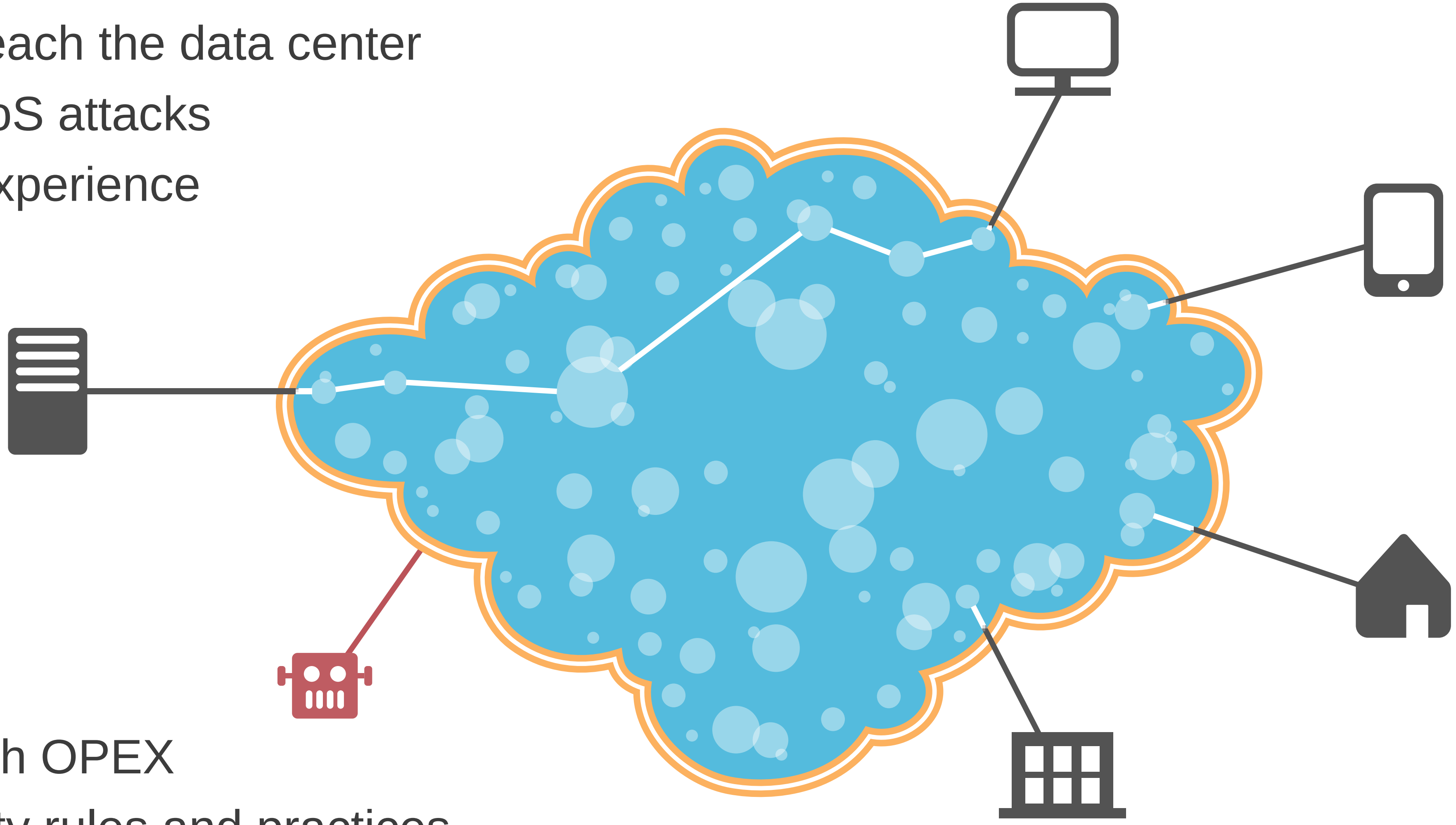
- **Layered defense** to DDoS new standard:
  - Strong perimeter defense (firewalls, IDS & IPS technologies etc)
  - Relationship & communication process with upstream ISP's
  - Akamai globally distributed cyber attack defense network
- Integrating Multiple Vendors & Technologies
  - Integrate into **Disaster Recovery Plan/ Business Continuity plan**
  - Test regularly with relevant vendors and internal teams
  - Deal with attacks using the most appropriate location…

Best results achieved through planning & testing

Cloud: The Right Service Delivery Model

Platform

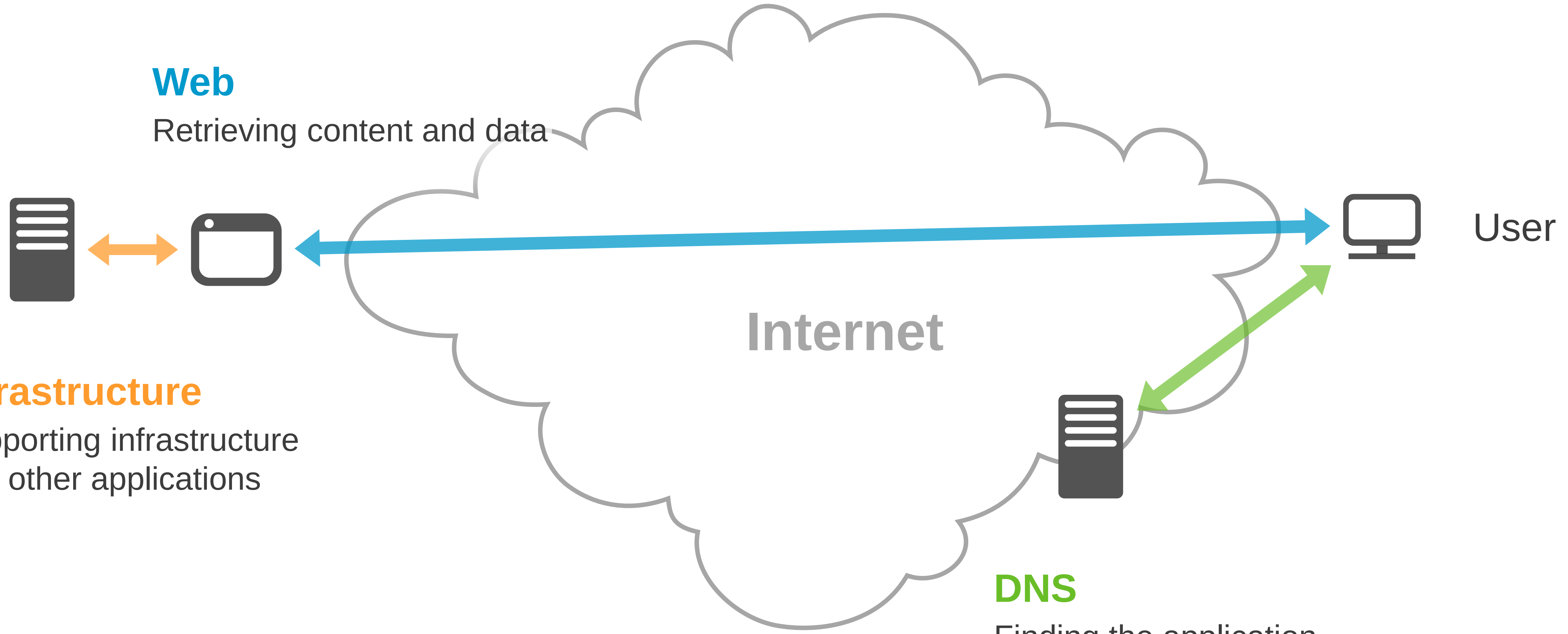
- Stop attacks before they reach the data center
- Grows with the size of DDoS attacks
- Provide world-class web experience



Service

- Replace upfront CAPEX with OPEX
- Continuously refined security rules and practices
- Access to Akamai resources and expertise

Multiple Perimeters for Internet-Facing Applications



Web

Retrieving content and data

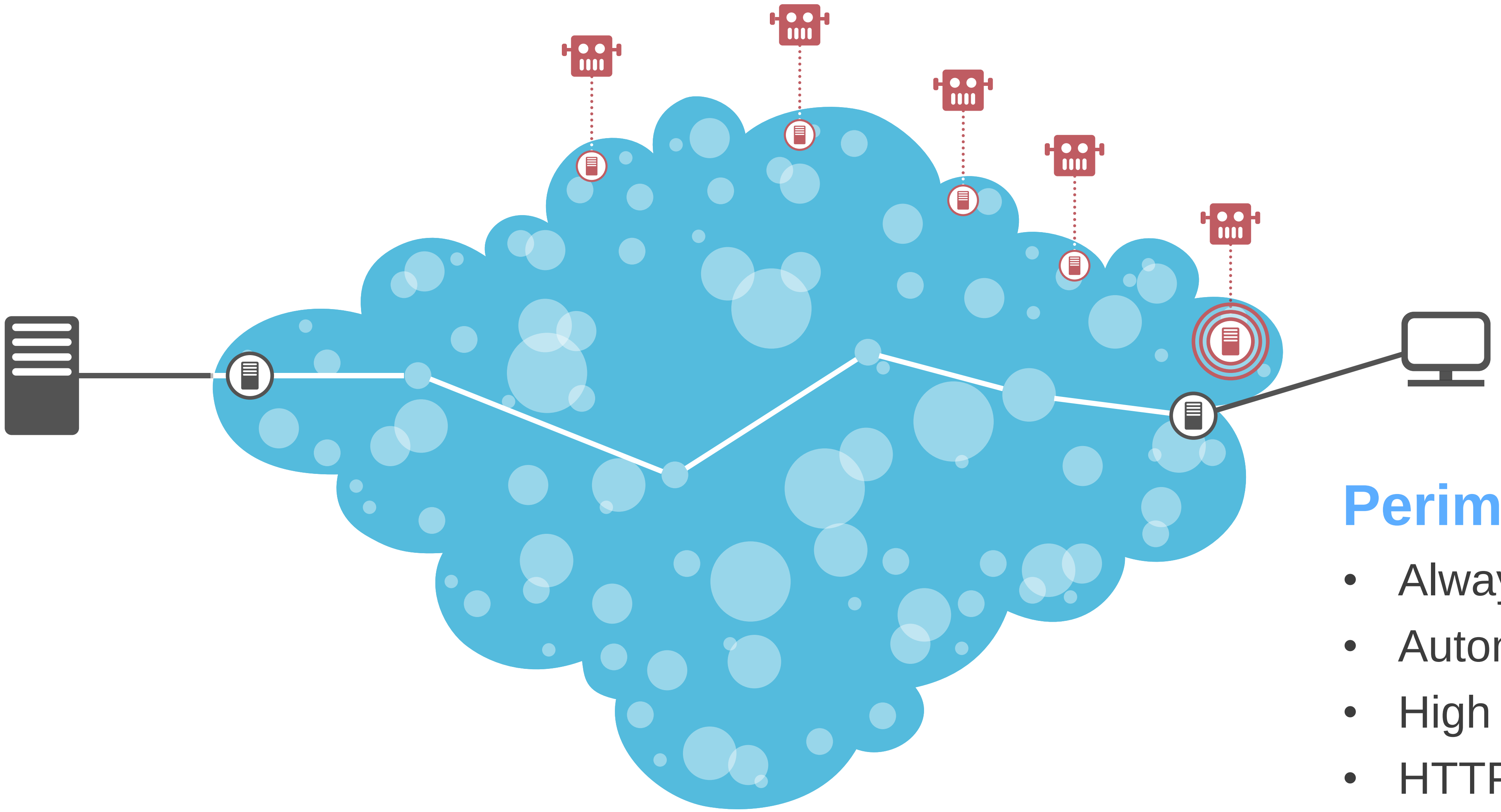
Infrastructure

Supporting infrastructure
and other applications

DNS

Finding the application

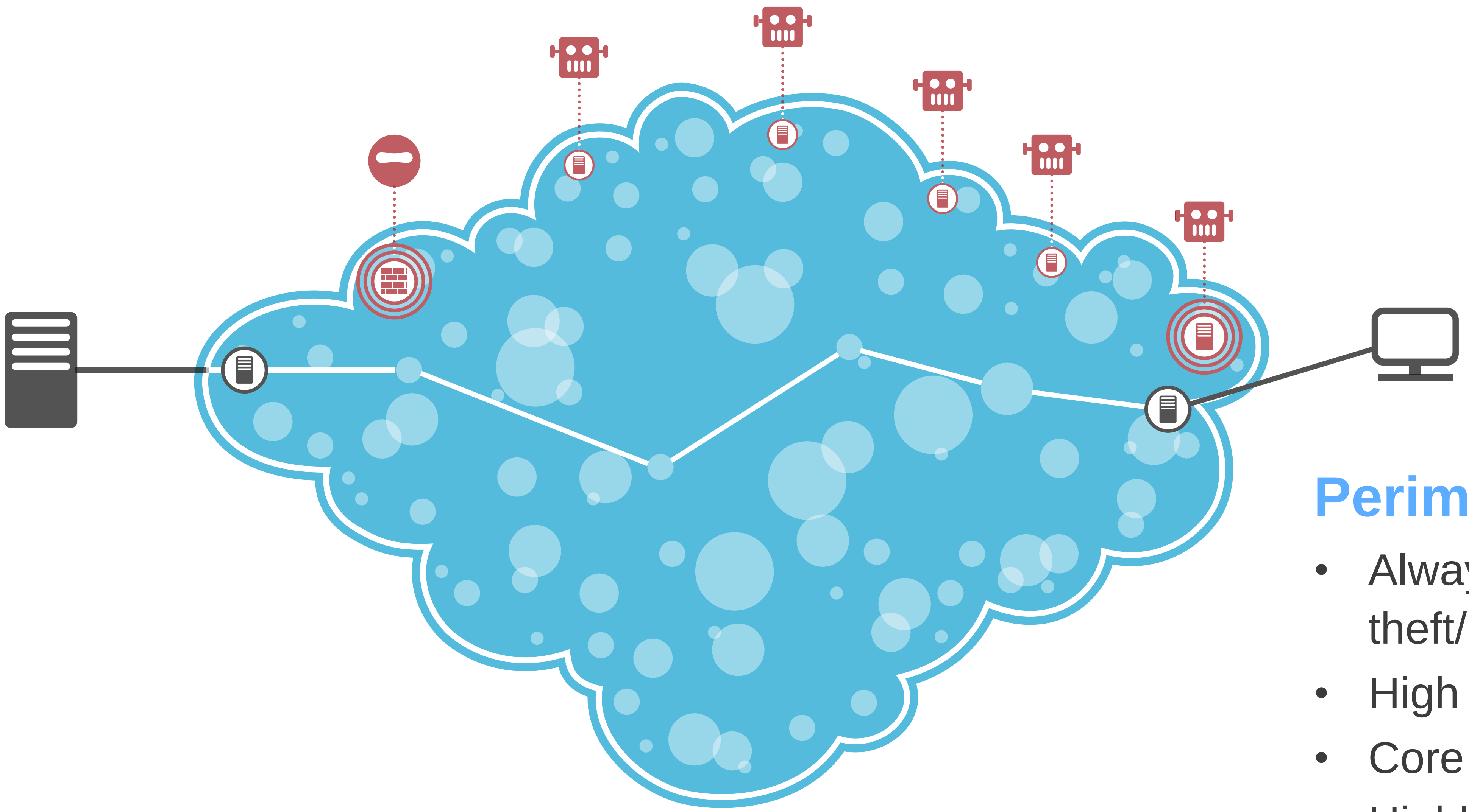
Protecting Multiple Perimeters in the Cloud



Perimeter 1 – Web (DDoS)

- Always-on defense
- Automated (rate controls, caching)
- High performance
- HTTP / HTTPS (Port 80/Port 443)
- Local or cloud-based applications

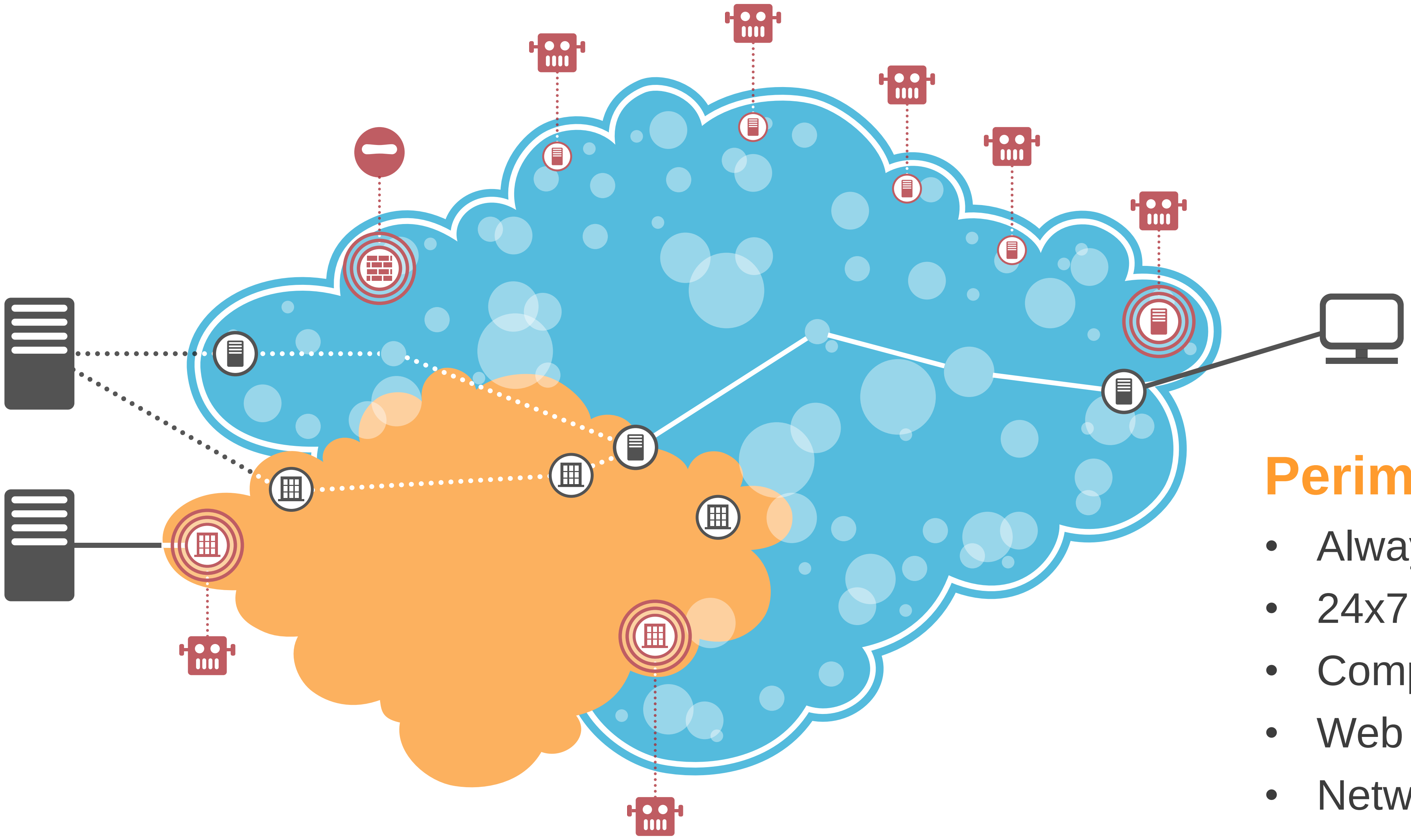
Protecting Multiple Perimeters in the Cloud



Perimeter 2 – Web (WAF)

- Always-on defense against data theft/breach/scraping
- High performance and scalability
- Core Rule Set + Kona Rule Set
- Highly accurate (reduced FP, FN)
- HTTP / HTTPS
- Local or cloud-based applications

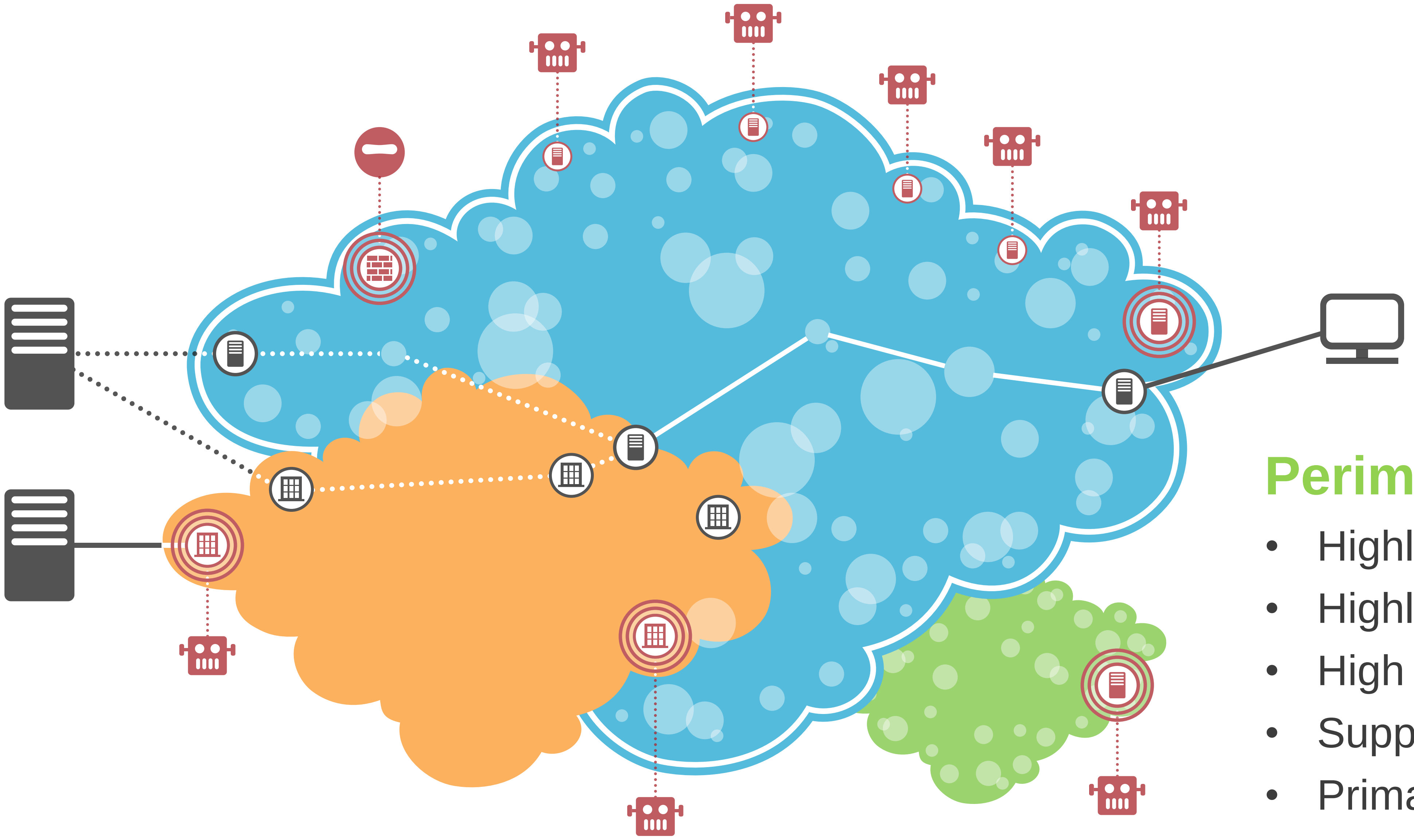
Protecting Multiple Perimeters in the Cloud



Perimeter 3 – Origin (DDoS)

- Always-on or on-demand
- 24x7 SOC (5-20 min SLA)
- Comprehensive (subnet granularity)
- Web and IP applications
- Network infrastructure + bandwidth
- ASN, Class-C, BGP Routers

Protecting Multiple Perimeters in the Cloud



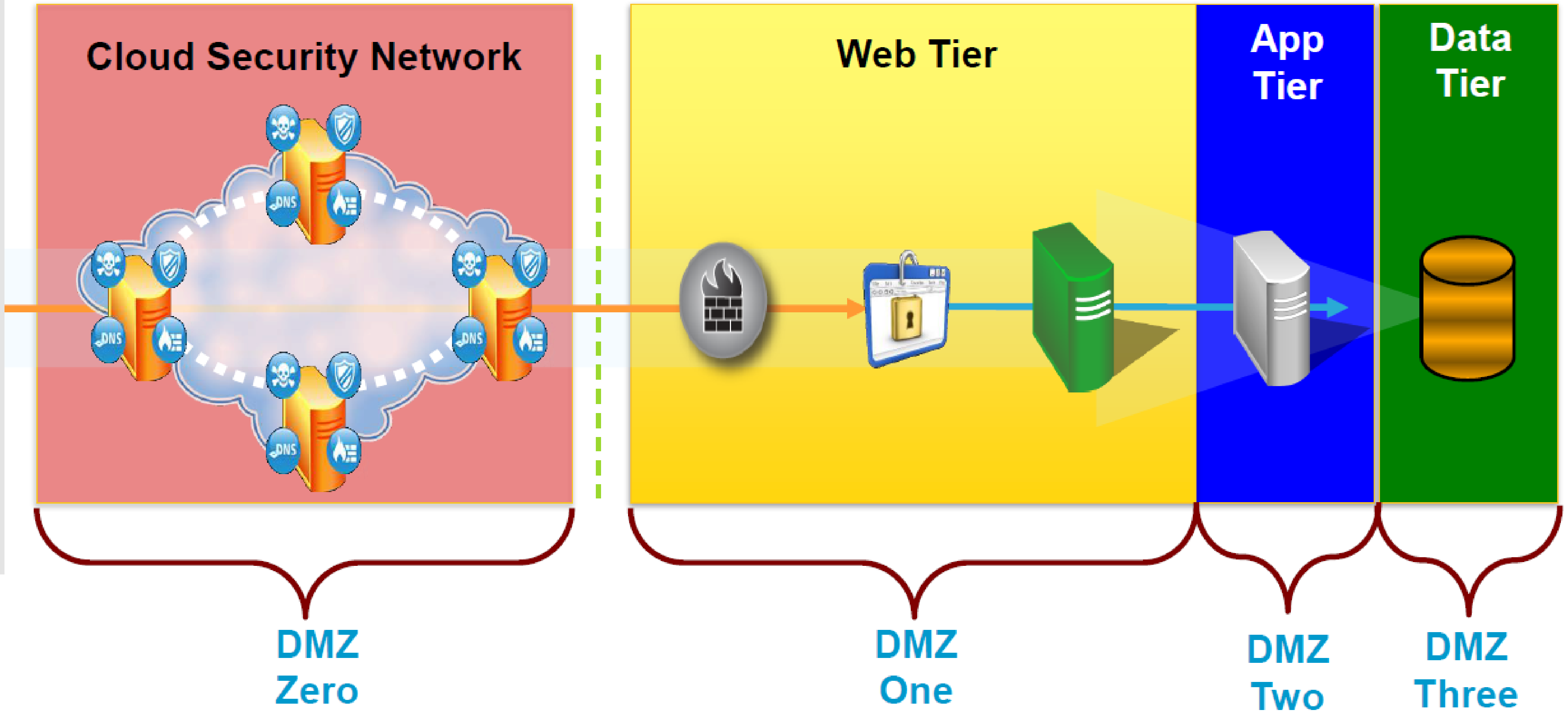
Perimeter 4 – DNS

- Highly scalable (<1% total capacity)
- Highly available (24x7 SLA)
- High performance (zone apex)
- Supports DNSSEC
- Primary and secondary DNS

Layered Defense to Protect

Cloud Security Network – DMZ Zero

1. Perimeter 1 – Web (DDoS)
2. Perimeter 2 – Web (WAF)
3. Perimeter 3 – Origin (DDoS)
4. Perimeter 4 – DNS



How to evaluate Cloud Security Service Providers

1. **Threat Intelligence**
   - Do you have an internal DDoS threat intelligence research group?
   - What threat intelligence do you publish and provide to your customers?
2. **Front-line Experiences**
   - How many years have you been providing DDoS protection service to the public?
   - Do you have a large customer base supporting the cost of network and mitigation capacity growth?
3. **Mitigation Capabilities**
   - What methods of traffic redirection do you support?
   - Do you have options for both on-demand and always-on DDoS service options?
   - Can you protect my DNS servers even if they are located in a third-party hosted environment?
   - Do you provide a time-to-mitigate Service Level Agreement (SLA)?
   - Do you provide any cloud security services beside DDoS?
   - What types of attacks have you successfully mitigated?
   - Do you offer a fully managed DDoS service? How do you drive the mitigation strategy?
   - What types of redundancies are provided in each one of your network and mitigation platforms?
4. **Mitigation Capacity**
   - What is the network and mitigation capacity for each one of your protection platforms?
   - Are there any fixed caps or fees associated with attack size or number of attacks?
   - How is your network and mitigation capacity distributed across the globe? Does the service use Anycast or a similar technology to distribute the attack traffic across multiple locations?
   - Have you ever experienced a network outage due to a DDoS attack?
   - What is the largest attack you've ever mitigated successfully on each of your protection platforms?
   - Have you ever denied service due to defending multiple simultaneous attacks?

Akamai

FASTER FORWARD

Q & A

wlock@akamai.com
Mobile: 63896000