Ferramentas de Ataques de DDoS e a Evolução de ameaças a disponibilidade contra serviços Internet

Julio Arruda

Gerente America Latina – Engenharia

Agenda

- The Affect of DDoS on Business
- DDoS Statistics, Motivations and Tools
- Understanding DDoS
- Protecting Your Network Against the DDoS Threat

Distributed Denial of Service (DDoS)

Filling up your network capacity

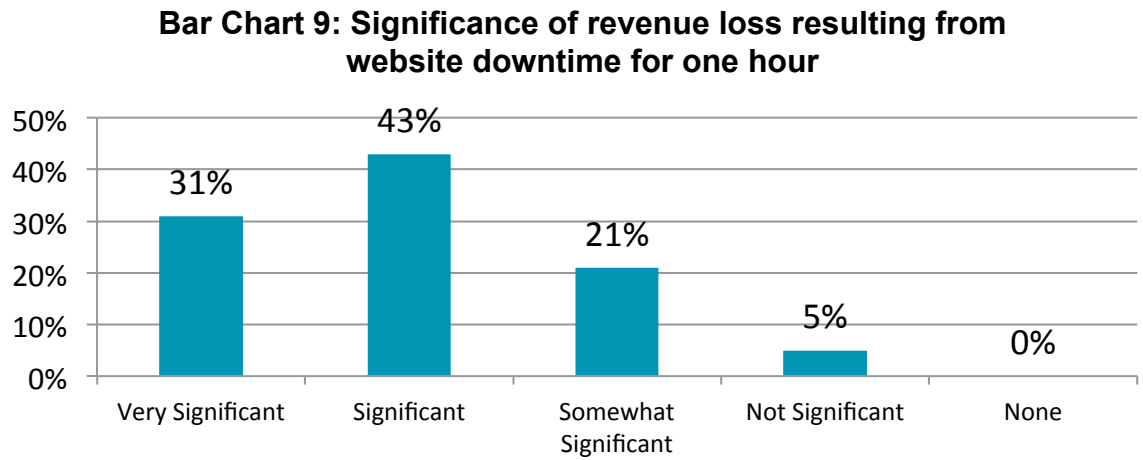
ARBOR NETWORKS

Direct Effects of DDoS

- Internet services off-line!
- Internet services slowed to a crawl!
- Database congested!
- Internet connection down!
- Network infrastructure overwhelmed!
- DNS down!
- VOIP down!
- Email down!
- Gaming Server down!

ARBOR NETWORKS

Impact of DDoS Attacks on the Business



Source: Ponemon Institute – 2010 State of Web Application Security

Botnets & DDoS attacks cost an *average* enterprise *$6.3M for a 24-hour outage!**

* Source: McAfee – Into the Crossfire – January 2010

The impact of loss of service availability goes beyond financials:

Operations	Help Desk	Recovery	Lost Worker Output	Penalties	Lost Business	Brand & Reputation Damage
How many IT personnel will be tied up addressing the attack?	How many more help desk calls will be received, and at what cost per call?	How much manual work will need to be done to re-enter transactions?	How much employee output will be lost?	How much will have to be paid in service level agreement (SLA) credits or other penalties?	How much will the ability to attract new customers be affected? What is the full value of that lost customers?	What is the cost to the company brand and reputation?

DDoS: It Will Happen To You

- Ostrich Mentality : ‘When an ostrich is afraid, it will bury its head in the ground, assuming that because it cannot see, it cannot be seen.’

- The attitude to DDoS as a **Service Availability Threat** has been similar.
- …but this is changing because of:
  - **AWARENESS :** Massive mainstream press around Anonymous, Lulzsec, Sony, etc..
  - **RISK :** Businesses are reliant on the Internet for their business continuity.
  - **MOTIVATIONS** : Wider spread of attack motivations, broader target set.
  - **EXPERIENCE :** Larger, more frequent, more complex attacks.

ARBOR NETWORKS

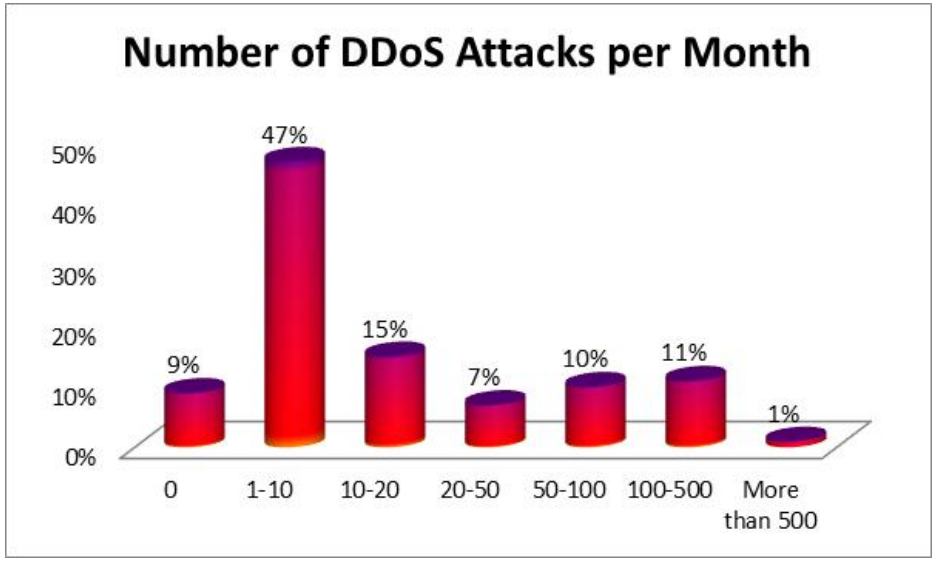
DDoS Statistics, Motivations and Tools

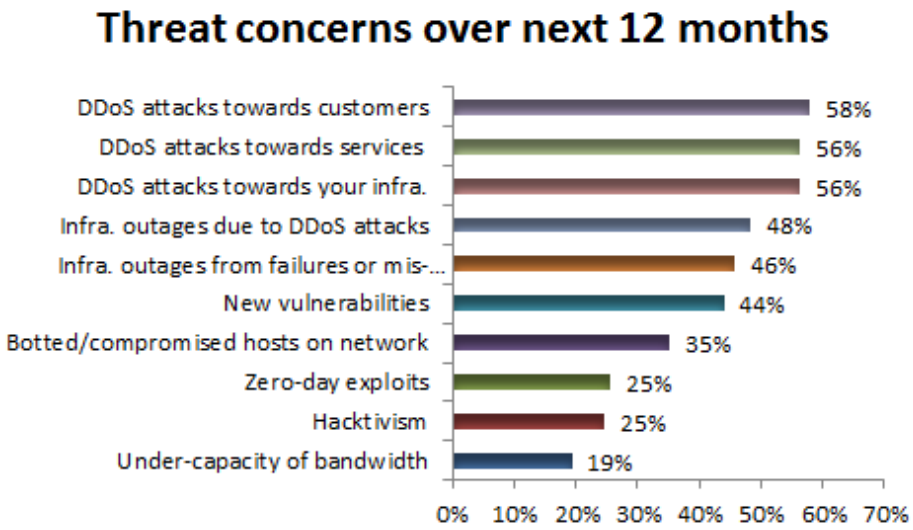
ARBOR NETWORKS

Arbor Research

- ASERT Botnet and DDoS Research
  - Analysis of hundreds of unique botnets and attack tools used to carry out DDoS attacks
- 2011 Worldwide Infrastructure Security Report
  - Survey of 114 Internet operators focused on security practices, incidents and trends
- ATLAS Data Trends
  - Data collected from 100+ Arbor deployments and honeynets sharing attack and traffic statistics

DDoS Attack Frequency Makes it Top of Mind



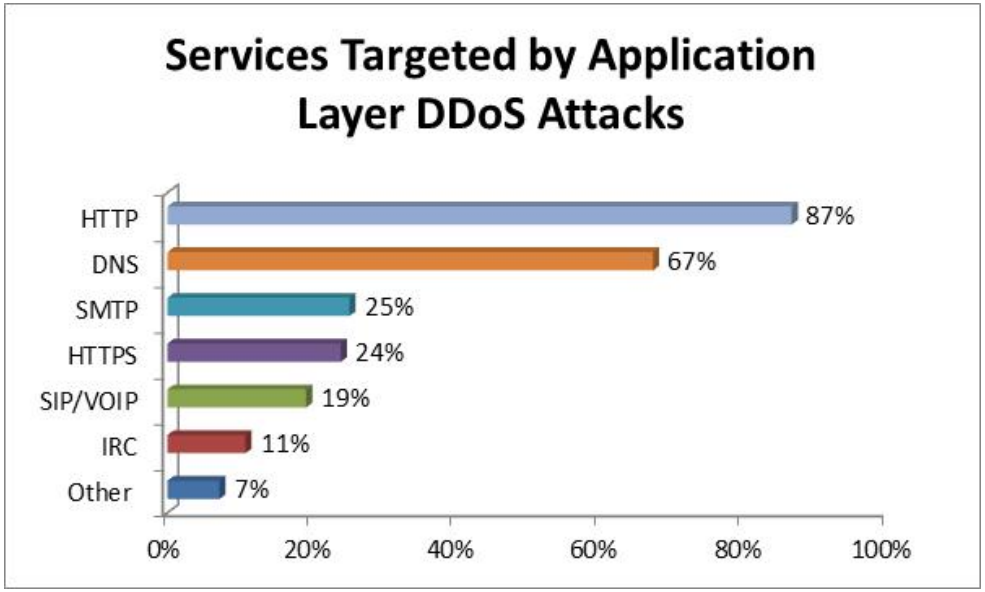


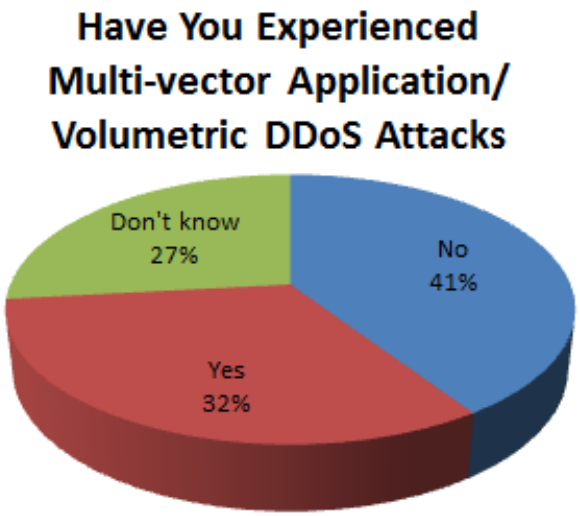
Source: Arbor Networks 2011 Infrastructure Security Report

- Distributed Denial of Service (DDoS) attacks are now a common occurrence across the Internet
- Top of mind topic for Internet Operators
- Anyone can become a victim

ARBOR NETWORKS

Application Layer and Multi-vector DDoS





- A higher percentage of attacks reported on HTTP and IRC relative to 2010
  - HTTP and IRC up relative to 2010
- Lower percent of attacks on DNS, SMTP, HTTPS and VOIP
- SSL based attacks reported included TCP and UDP floods against port 443, port scanning attempts and Slowloris

ARBOR NETWORKS

The DDoS Tool Landscape

- Many malware families have added DDoS capabilities
- Attackers now have hundreds of tools to choose from at varying costs and complexities
  - Single user flooding tools
  - Host booters
  - Shell booters
  - Remote Access Trojans (RATs)
  - DDoS bots of varying complexity

ARBOR NETWORKS

Single User Plus: LOIC

Low Orbit Ion Cannon | U dun goofed | v. 1.1.1.25

Low Orbit Ion Cannon

github.com/NewEraCracker/LOIC

Manual Mode (Do it yourself) IRC Mode (HiveMind)

IRC server | Port 6667 | Channel #loic | Disconnected.

1. Select your target

URL Lock on

IP Lock on

3. Ready?

IMMA CHARGIN MAH LAZER

Selected target

NONE!

2. Attack options

TCP / UDP message

U dun goofed

HTTP Subsite

/

Append random chars to the subsite / message

<= faster Speed slower =>

TCP | 80 | 10 | 9001

Method Port Threads Timeout

Wait for reply

Use Gzip (HTTP)

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

- "HiveMind" mode
- Still used despite revelation of attackers IP

ARBOR NETWORKS

Host booter – Silent-DDoSer

Silent-DDoSer 2.5 - [Private Beta]

Menu Connection Port

Zombies Online (3):	Server ID:	Country:	Version:	Operating System:	Status:
207.204.186.119	BETA 2.0	United States	2.0	Windows 7 x32	Idle...
79.158.157.199	BETA 2.0	Spain	2.0	Windows Vista x32	Idle...
82.72.135.184	BETA 2.0	Netherlands	2.0	Windows 7 x32	Idle...

Silent-DDoSer

Socket Status: 82.72.135.184 Connected... Peak: 3 Update/Download Progress:

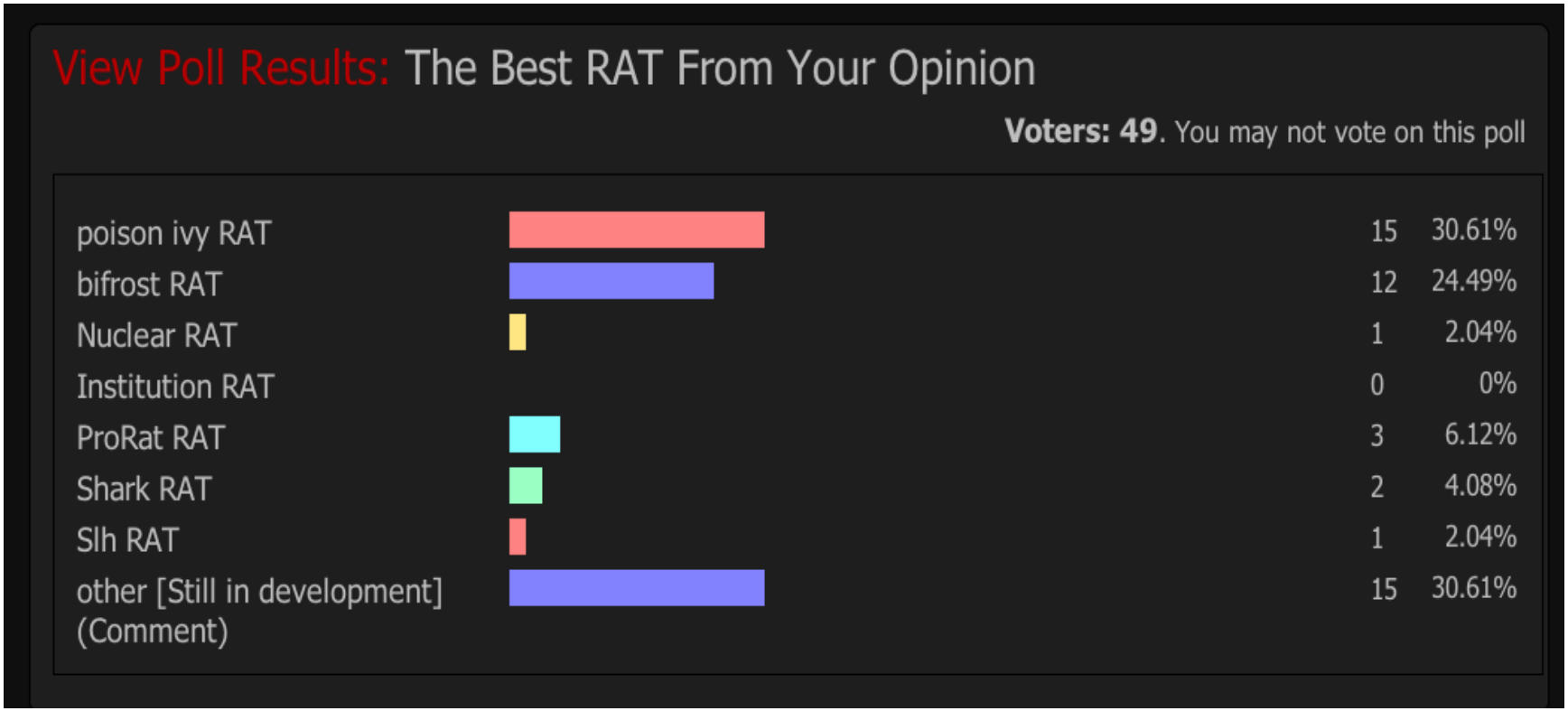
ARBOR NETWORKS

Shell Booters – twBooter

- 235 shells online
- Botmaster involved in online DDoS war

ARBOR NETWORKS

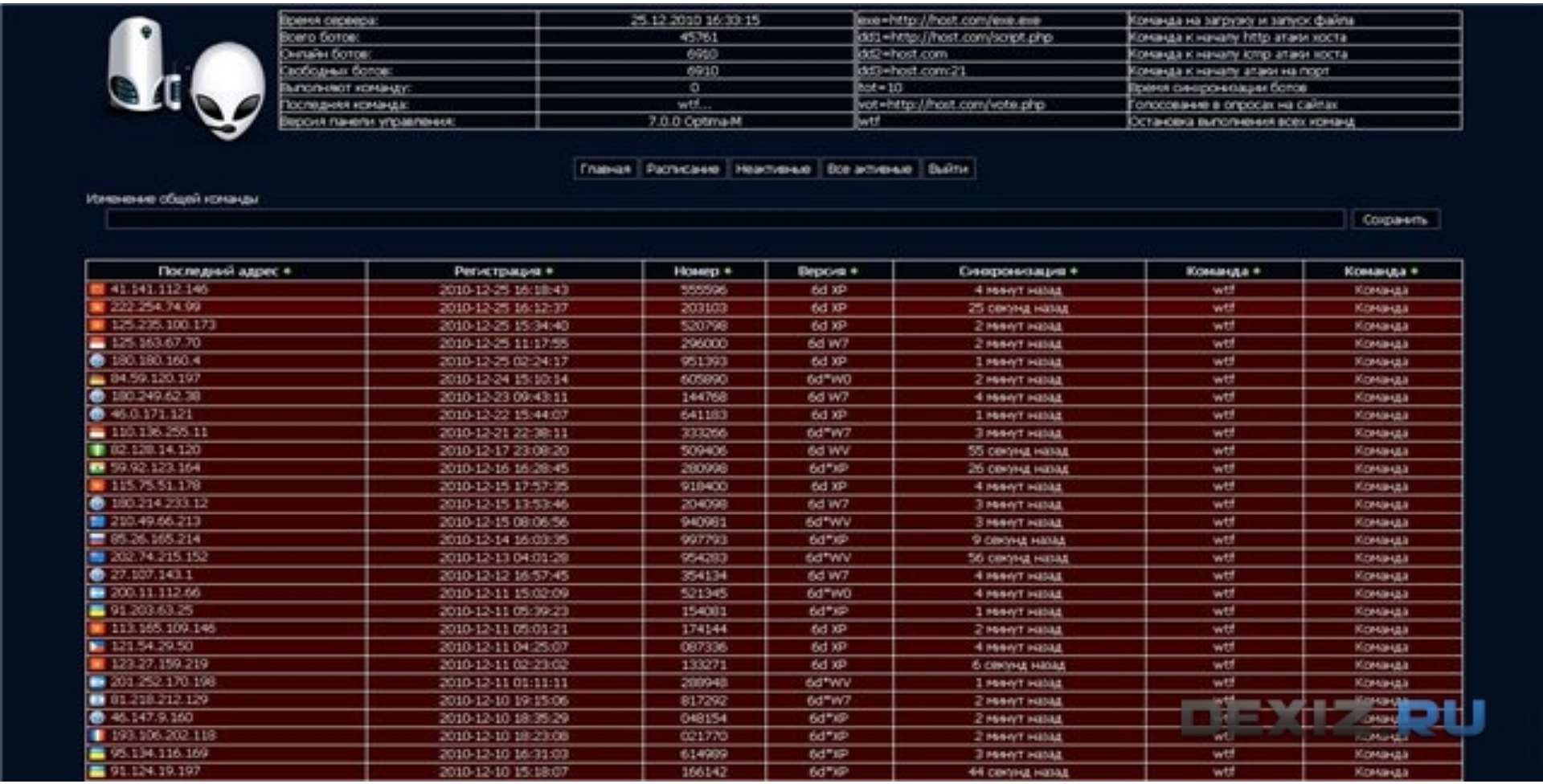
RATs Scurrying Everywhere



- Used by attackers of varying skill and motive
- Skilled attackers will aim for evasion
  - Gh0st RAT network signature changes
- Often packed with run-time decryption to evade anti-malware

ARBOR NETWORKS

Commercial DDoS Product - Darkness



Время сервера:	25.12.2010 16:33:15	exe=http://host.com/exe.exe	Команда на загрузку и запуск файла
Всего ботов:	45761	ddt1=http://host.com/script.php	Команда к началу http атаки хоста
Онлайн ботов:	6910	ddt2=host.com	Команда к началу icmp атаки хоста
Свободных ботов:	6910	ddt3=host.com:21	Команда к началу атаки на порт
Выполняют команду:	0	bot=10	Время синхронизации ботов
Последняя команда:	wtf...	vot=http://host.com/vote.php	Голосование в опросах на сайтах
Версия панели управления:	7.0.0 OptimaM	wtf	Остановка выполнения всех команд

Главная | Расписание | Неактивные | Все активные | Выйти

Изменение общей команды

Сохранить

Последний адрес	Регистрация	Номер	Версия	Синхронизация	Команда	Команда
41.141.112.146	2010-12-25 16:18:43	555596	6d XP	4 минут назад	wtf	Команда
222.254.74.99	2010-12-25 16:12:37	203103	6d XP	25 секунд назад	wtf	Команда
125.235.100.173	2010-12-25 15:34:40	520798	6d XP	2 минут назад	wtf	Команда
125.163.67.70	2010-12-25 11:17:55	296000	6d W7	2 минут назад	wtf	Команда
180.180.160.4	2010-12-25 02:24:17	951393	6d XP	1 минут назад	wtf	Команда
84.59.120.197	2010-12-24 15:10:14	605890	6d*W0	2 минут назад	wtf	Команда
180.249.62.38	2010-12-23 09:43:11	144768	6d W7	4 минут назад	wtf	Команда
46.0.171.121	2010-12-22 15:44:07	641183	6d XP	1 минут назад	wtf	Команда
110.136.255.11	2010-12-21 22:38:11	333266	6d*W7	3 минут назад	wtf	Команда
82.128.14.120	2010-12-17 23:08:20	509406	6d WV	55 секунд назад	wtf	Команда
59.92.123.164	2010-12-16 16:28:45	280998	6d*XP	26 секунд назад	wtf	Команда
115.75.51.178	2010-12-15 17:57:35	918400	6d XP	4 минут назад	wtf	Команда
180.214.233.12	2010-12-15 13:53:46	204098	6d W7	3 минут назад	wtf	Команда
210.49.66.213	2010-12-15 08:06:56	940981	6d*WV	3 минут назад	wtf	Команда
85.26.165.214	2010-12-14 16:03:35	997793	6d*XP	9 секунд назад	wtf	Команда
202.74.215.152	2010-12-13 04:01:29	954283	6d*WV	56 секунд назад	wtf	Команда
27.107.143.1	2010-12-12 16:57:45	354134	6d W7	4 минут назад	wtf	Команда
200.11.112.66	2010-12-11 15:02:09	521345	6d*W0	4 минут назад	wtf	Команда
91.203.63.25	2010-12-11 05:39:23	154081	6d*XP	1 минут назад	wtf	Команда
113.165.109.146	2010-12-11 05:01:21	174144	6d XP	2 минут назад	wtf	Команда
121.54.29.50	2010-12-11 04:25:07	087336	6d XP	4 минут назад	wtf	Команда
123.27.159.219	2010-12-11 02:23:02	133271	6d XP	6 секунд назад	wtf	Команда
201.252.170.198	2010-12-11 01:11:11	289948	6d*WV	1 минут назад	wtf	Команда
81.218.212.129	2010-12-10 19:15:06	817292	6d*W7	2 минут назад	wtf	Команда
46.147.9.160	2010-12-10 18:35:29	048154	6d*XP	2 минут назад	wtf	Команда
193.106.202.118	2010-12-10 18:23:08	021770	6d*XP	2 минут назад	wtf	Команда
95.134.116.169	2010-12-10 16:31:03	614989	6d*XP	3 минут назад	wtf	Команда
91.124.19.197	2010-12-10 15:18:07	166142	6d*XP	44 секунд назад	wtf	Команда

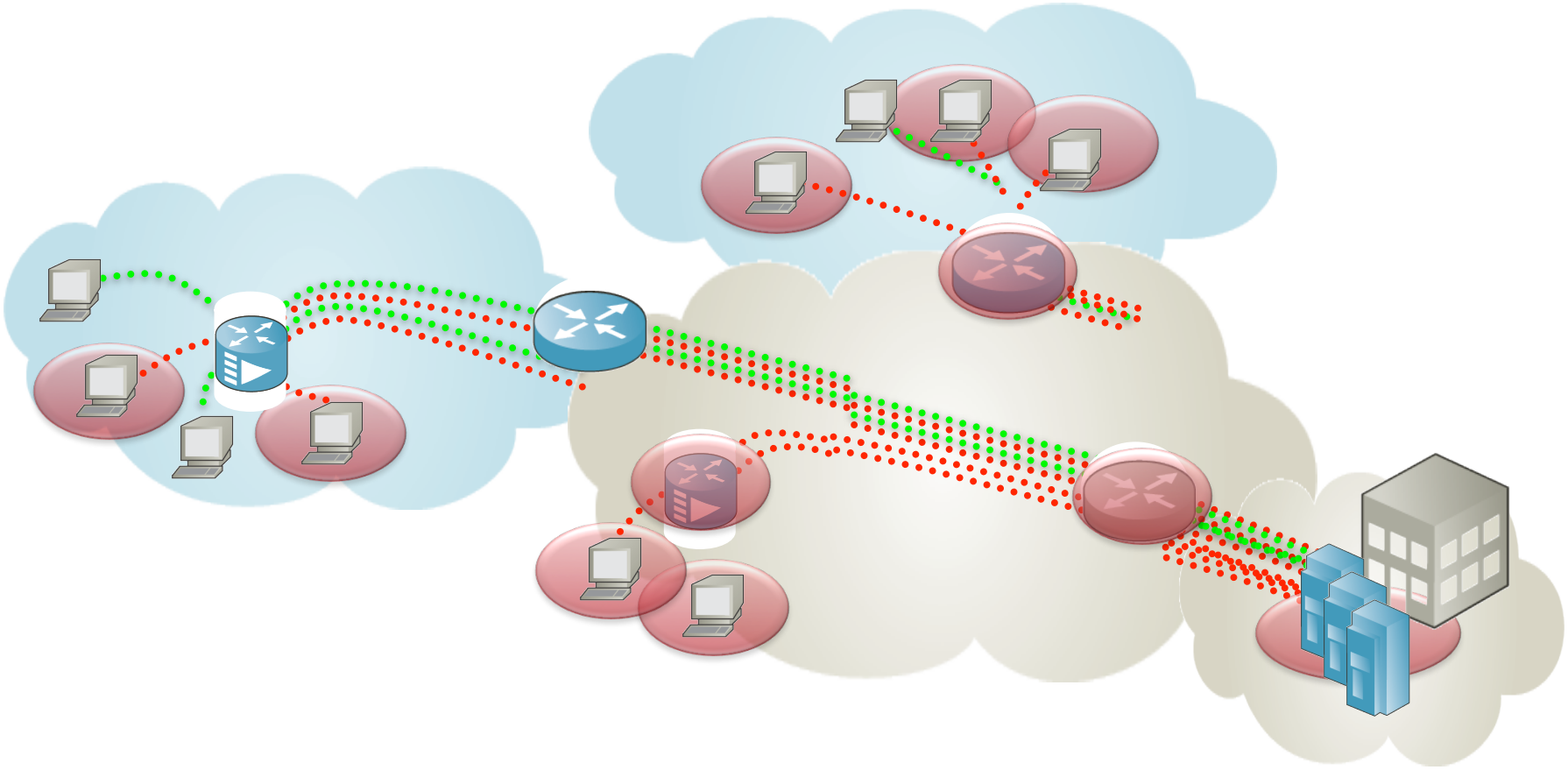
- 45,000 bots, 6900 online

ARBOR NETWORKS

Understanding DDoS

ARBOR NETWORKS

What is a DDoS Attack?



During a **Distributed Denial of Service (DDoS) attack**, compromised hosts (**bots)** or vigilante users from distributed sources overwhelm the target with illegitimate traffic so that the servers can not respond to legitimate clients.

High Bandwidth Volumetric DDoS

Description
Large volume of traffic in bps and/or pps. Traffic could be spoofed or not spoofed.
Effect on Network
Network links become saturated. Software based routers, switches, firewalls, IPS get overwhelmed.
Effect on Services
Legitimate users can't get to services.
Common Names
Packet flood, UDP flood, TCP flood.

ARBOR NETWORKS

Protocol Attacks

Description
Attacks that exploit vulnerable parts of protocols such as TCP 3 way handshake. They are often crafted to overwhelm protocol state on devices.
Effect on Network
State tables on servers, load balancers, IPS and firewalls fill up and they will no longer pass traffic.
Effect on Services
Legitimate users can't get to services.
Common Names
SYN flood, RST flood, FIN flood

ARBOR NETWORKS

Connection Based Attacks

Description
Attackers create many connections to the service sending no traffic or infrequent traffic. Sometimes the attacker may send incomplete requests to the services.
Effect on Network
Available connections to the service are exhausted. State tables of FW, IPS, load balancers could also get overwhelmed.
Effect on Services
Legitimate users can't connect to services.
Common Names
Sockstress

Reflection Attacks

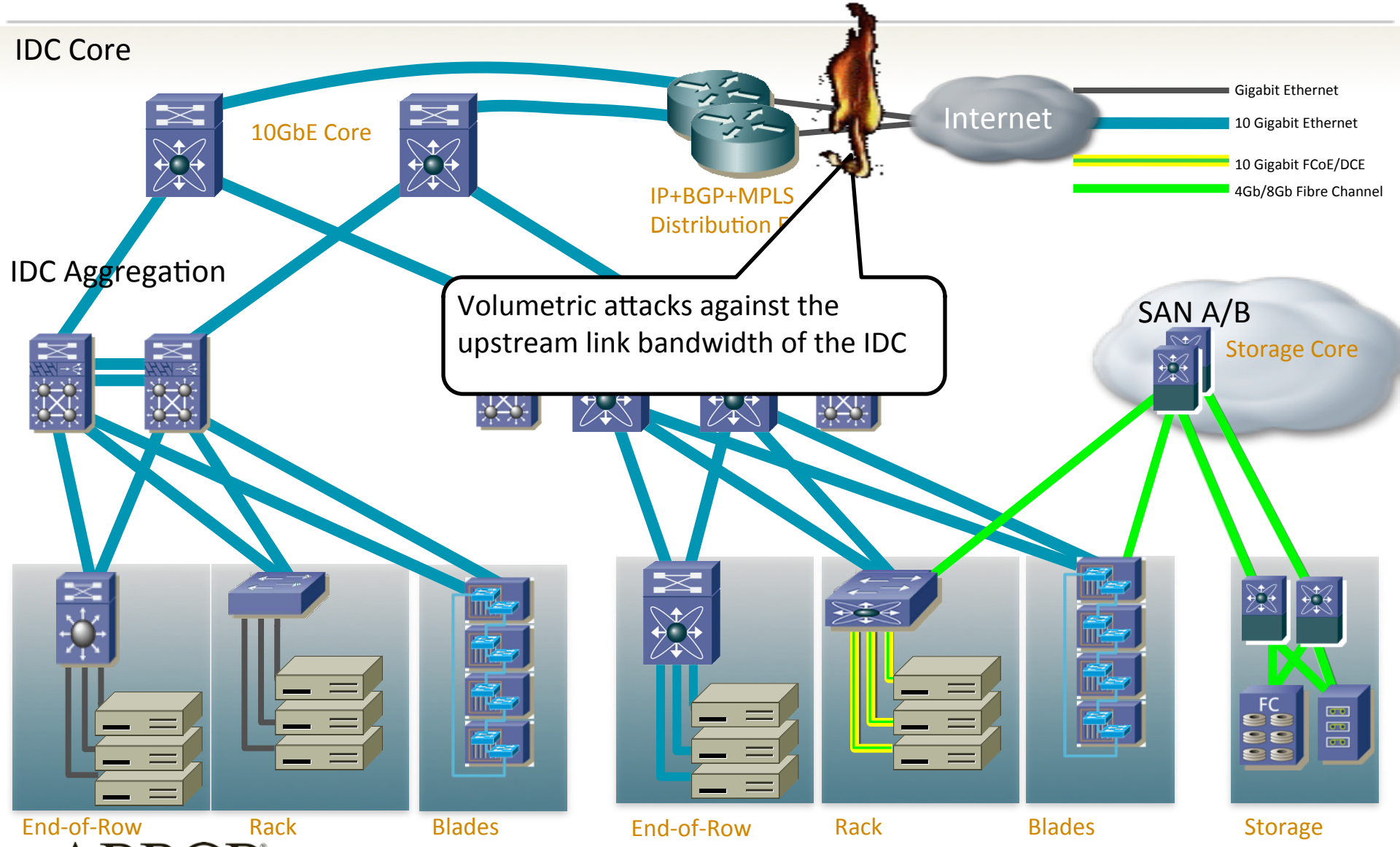
Description
Attackers spoof IP address of victim as source and send queries to open proxies or resolvers that will then send "answers" to the victim. Answers may be amplified if the response is bigger
Effect on Network
Network links become saturated. Software based routers, switches, firewalls, IPS get overwhelmed.
Effect on Services
Legitimate users can't get to services.
Common Names
DNS reflection, DNSSec amplification

ARBOR NETWORKS

Application-Layer Attacks

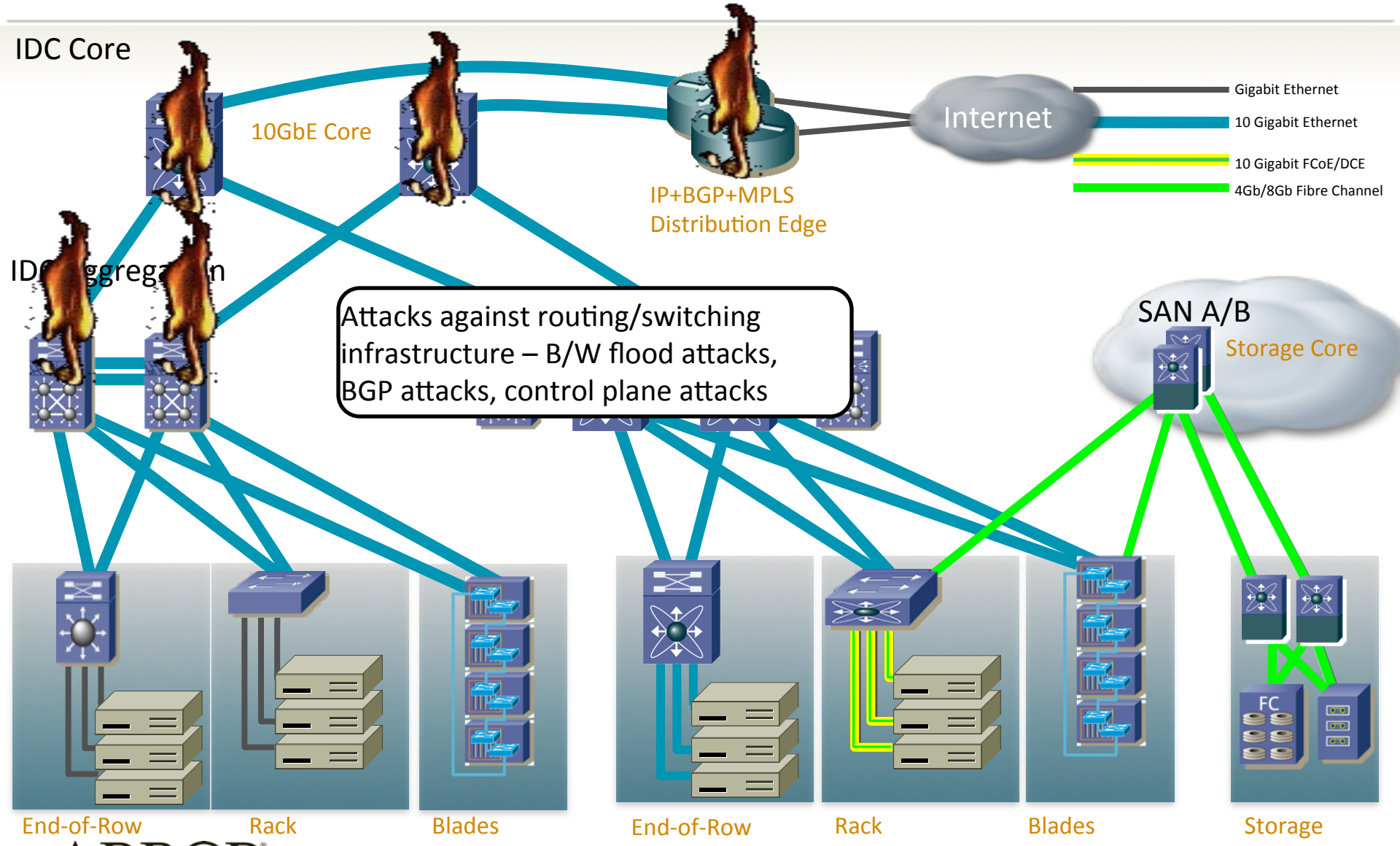
Description
Attacks that target a vulnerability at the application layer. They can range from application floods to slow stealthy attacks that target a particular weakness.
Effect on Network
Limited network effect as the traffic rates can be very low. They sometimes cause congestion between services and storage databases.
Effect on Services
Services become unresponsive or go down altogether.
Common Examples
URL floods, R U Dead Yet (Rudy), Slowloris, LOIC, HOIC, DNS dictionary attacks

DDoS and the Datacenter Attack Surface



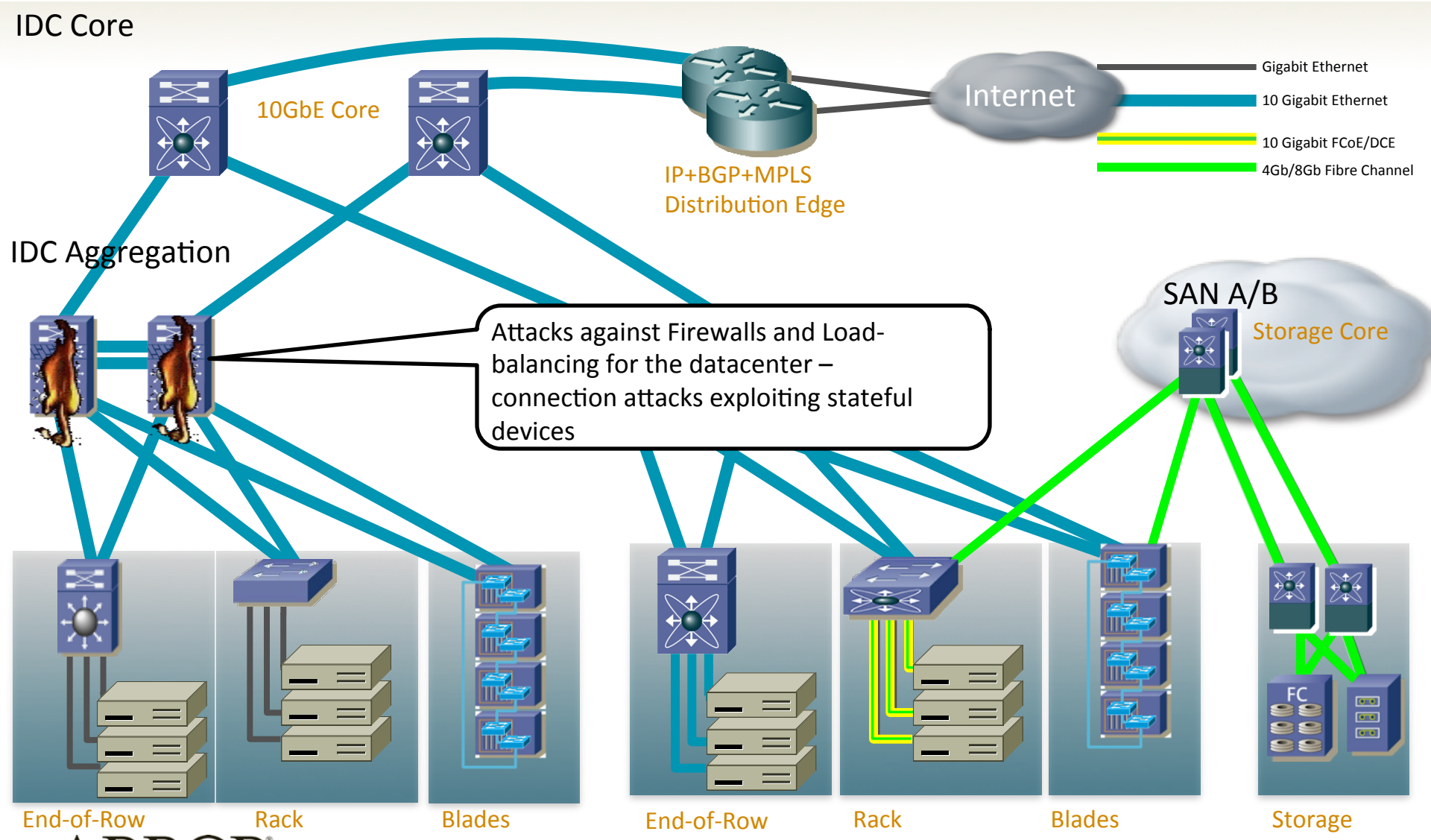
ARBOR NETWORKS

DDoS and the Datacenter Attack Surface



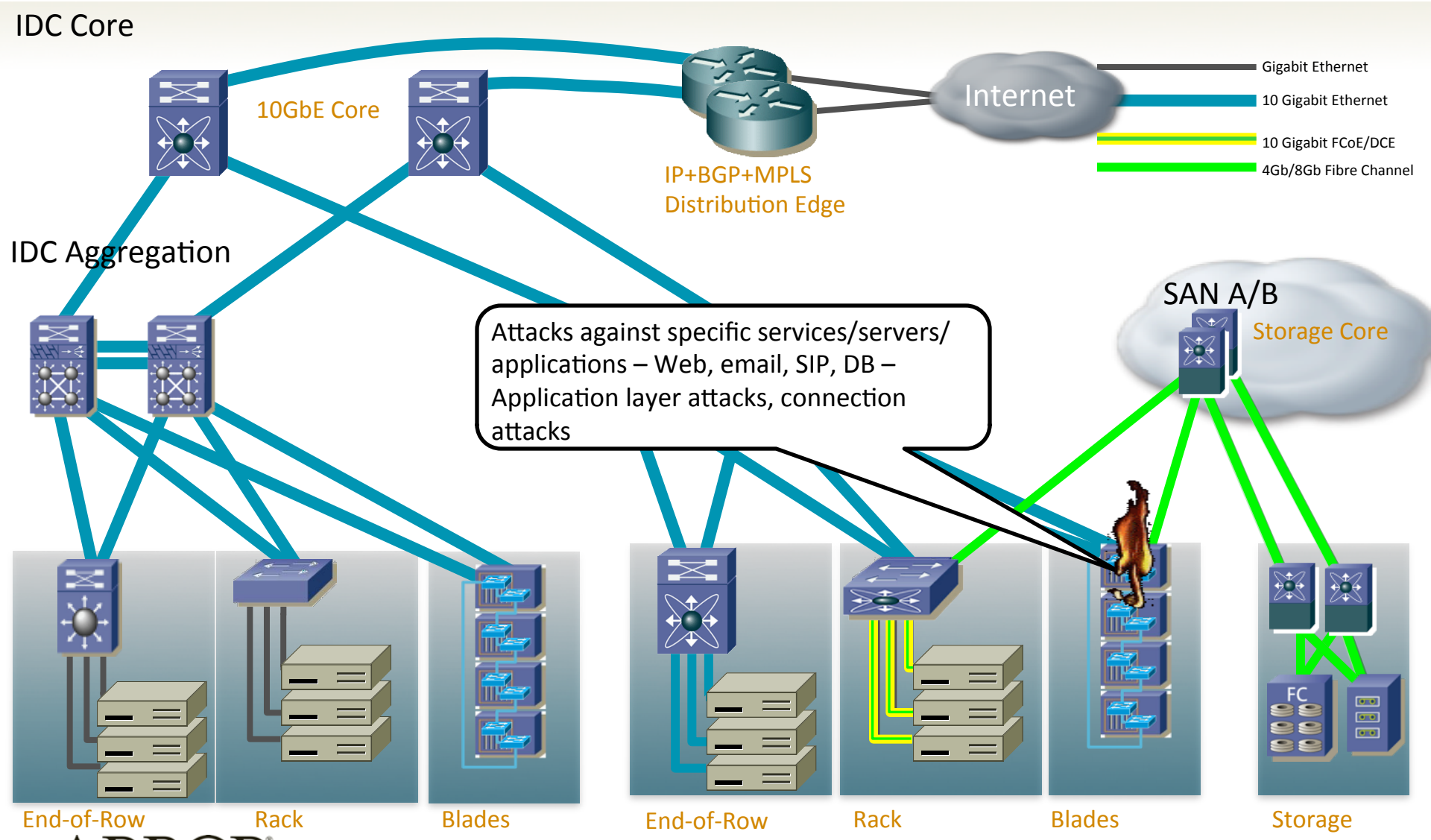
ARBOR NETWORKS

DDoS and the Datacenter Attack Surface



ARBOR NETWORKS

DDoS and the Datacenter Attack Surface



ARBOR NETWORKS

How to Protect Against DDoS

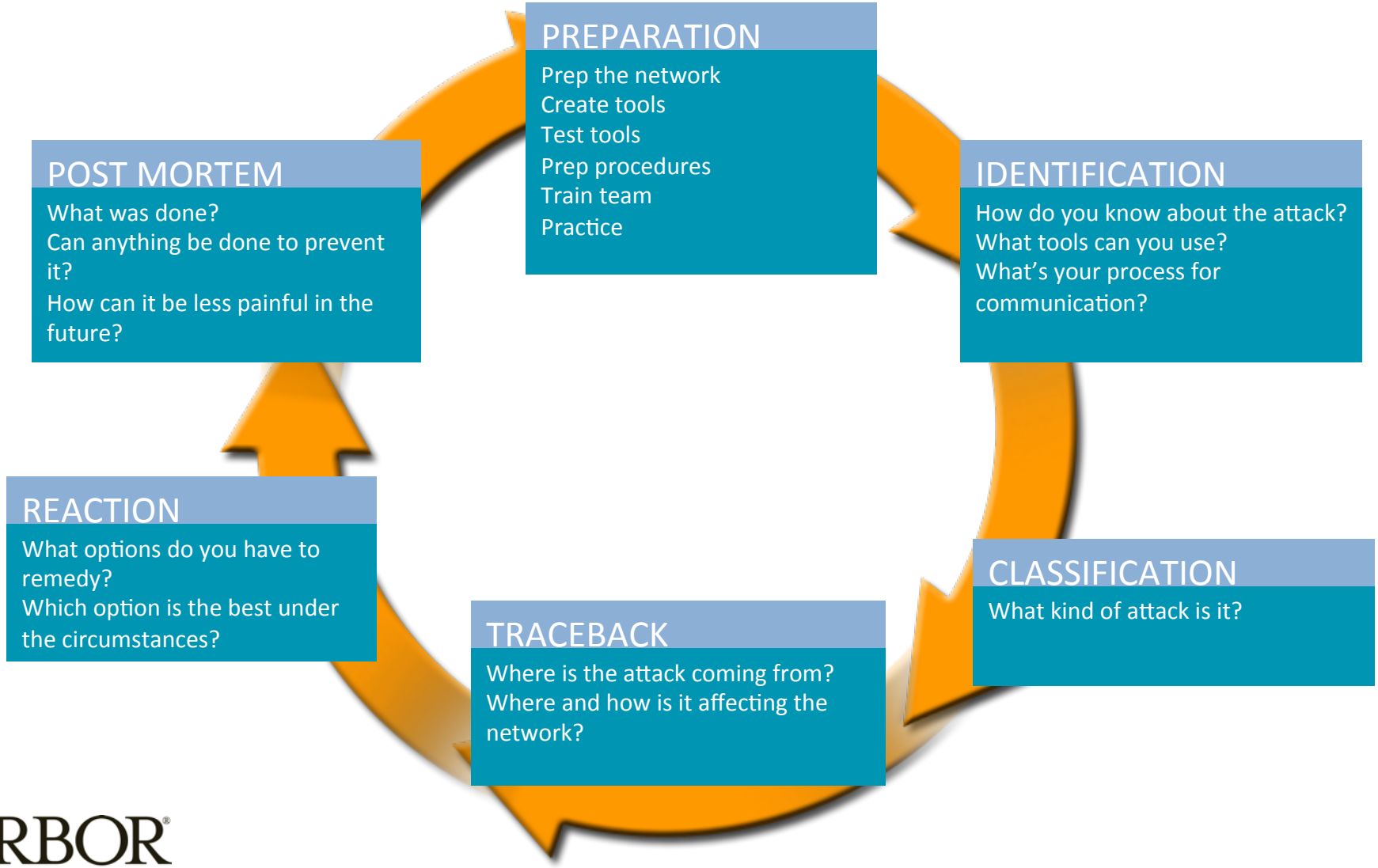
ARBOR NETWORKS

A Solution Needs to Handle All Attack Types

Different defenses are needed for different types of threats

ARBOR NETWORKS

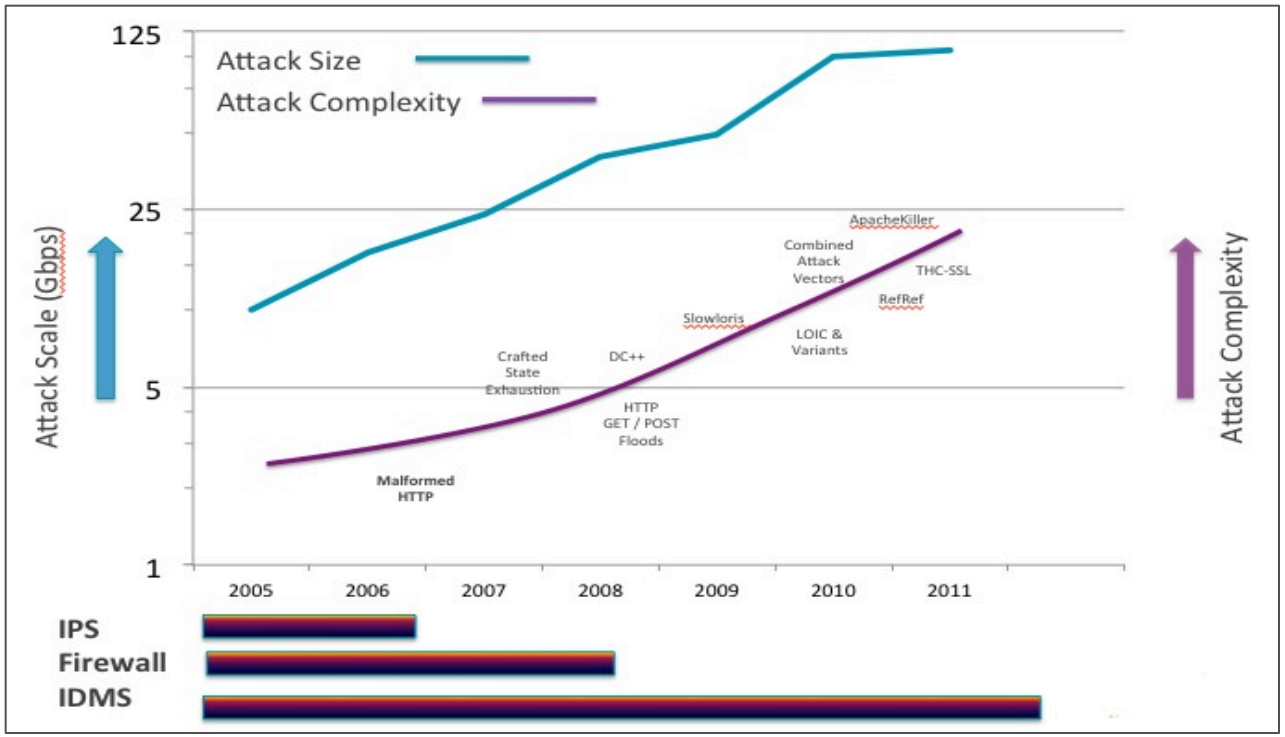
Six Phases of Infrastructure Security



ARBOR NETWORKS

DDoS Overwhelming Traditional Defenses

- Current DDoS attacks are designed to thwart general defenses
  - Use large, distributed botnets
  - Employ low-and-slow application layer attacks
  - Combine the above for obfuscation

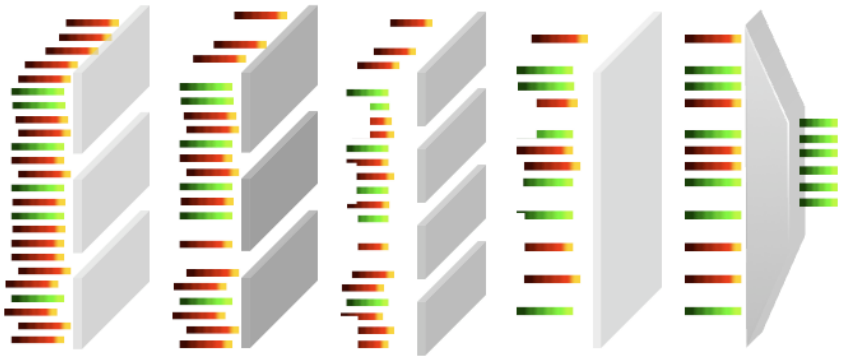


ARBOR NETWORKS

Intelligent DDoS Mitigation Systems

Stop advanced attacks including *application-layer* DDoS attacks using multiple counter-measures

- Block common and complex attacks using a variety of counter-measures such as the ones listed here
- Detect and stop application-layer DDoS attacks that are hard to detect in the cloud

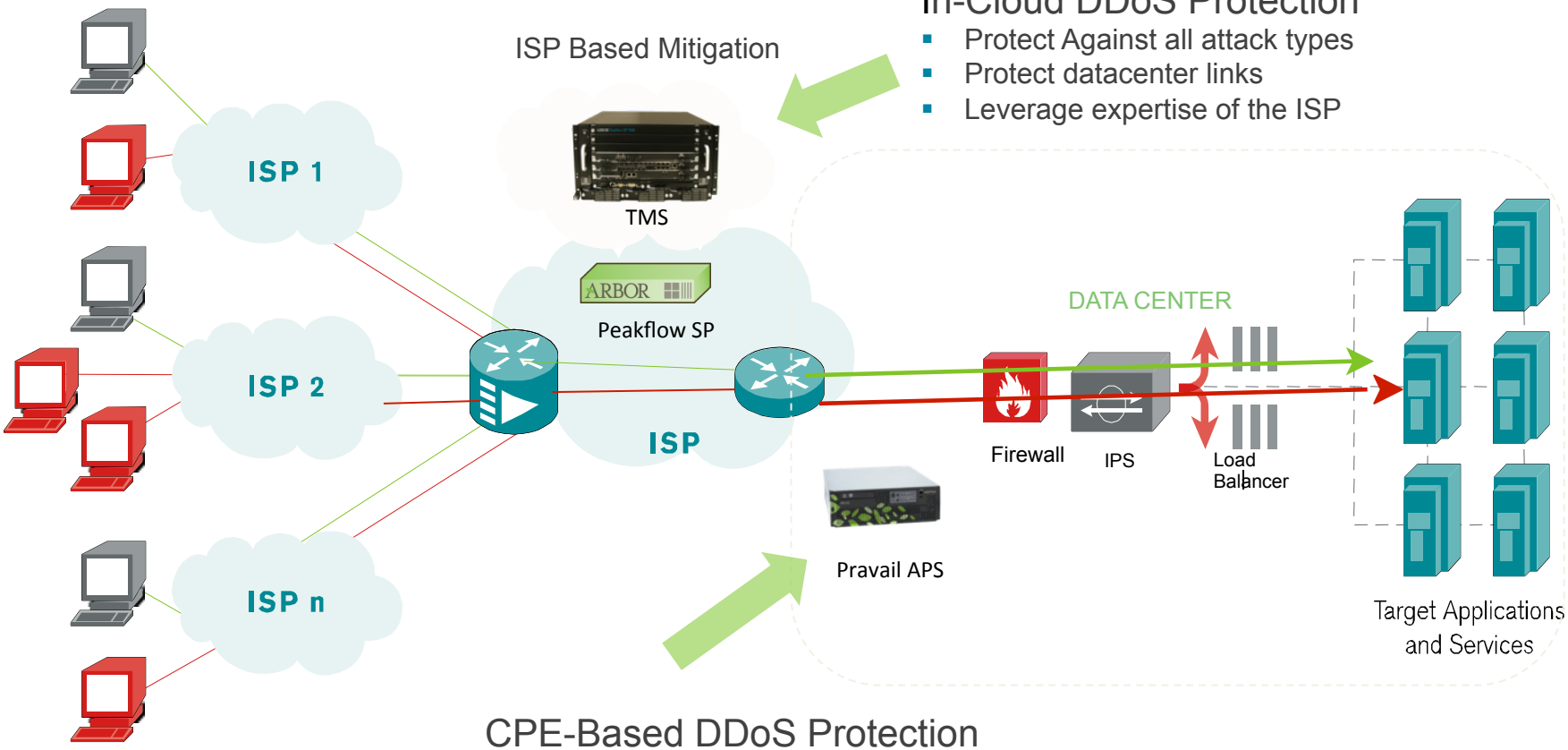


Multiple dimensions of counter-measures can be leveraged to stop dynamic and diverse threats

General
Single Source Attack
Distributed DDoS
Spoofed / Non-Spoofed Attacks
TCP Attacks
TCP SYN Floods
Invalid TCP Flag Combinations
Window Size Attacks (Sockstress, etc)
Slow TCP Connections (TCP Idling, etc)
HTTP / Web Attacks
Slow HTTP Connections (Slowloris / Pyloris)
HTTP GET / POST URL Floods
DNS
DNS Floods
DNS Authentication
Other
UDP / ICMP Floods
IP / TCP / UDP Fragment Floods
IP NULL Floods

ARBOR NETWORKS

Arbor's Intelligent, Layered DDoS Protection Solution



In-Cloud DDoS Protection

- Protect Against all attack types
- Protect datacenter links
- Leverage expertise of the ISP

CPE-Based DDoS Protection

- Always On Protection
- Keep services running when attacked
- Cloud signal to ISP system when overwhelmed

ARBOR NETWORKS

Case Study:
September 2012 Financial Sector Attacks

ARBOR NETWORKS

The beginning of “Operation Ababil”

- "Cyber fighters of Izz ad-din Al qassam” posted a call to action on Pastebin on September 18, calling for Muslims to attack the Bank of America and the New York Stock Exchange
- Four days earlier, messages linked to the same group called for attacks against Google's YouTube citing their refusal to take down a movie that offended some Muslims
- These attacks have continued several weeks towards varying targets

Attacks Take Major Financials Off-line

Major U.S. banks still under DDoS attack

Posted on 28 September 2012.

BOOKMARK

PNC Bank seems to be the latest target of the organized DDoS attacks agains major U.S. financial institutions such as JPMorgan Chase, Bank of America, Wells Fargo, Citigroup, U.S. Bancorp, New York Stock Exchange and others.

In the week, the banks' websites have b
bombarded with a flood of requests that
unable to reach them and perform finan
banking.

According to the statement posted onlin
Din al-Qassam Cyber Fighters group, th
forcing the takedown of the controversia
the group, mocks the prophet Muhamm

The hacktivists have also provided links
visited by volunteers, automatically use
aforementioned sites with requests.

Chase, NYSE Websites Targeted in Cyber Attacks

By Matt Egan, Adam Samson / Published September 19, 2012 / FOXBusiness

se (JPM) and NYSE Euronext (NYX) experienced
ednesday after being targeted by apparent cyber
lems come a day after Bank of America experienced
following a separate attack.

rs, an intelligence gathering network specializing in
d it believes the Chase outage is "likely due to a
of service attack." A Flashpoint analyst told FOX
ck was probably caused by "a large botnet," a tactic
y hacking group Anonymous. Generally, botnets
lling a large number of computers that have been

CNET › News › Security & Privacy › Wells Fargo is latest bank to be hit ...

Wells Fargo is latest bank to be hit by cyberattacks

As several banks experience outages, one group claims responsibility, saying it's retaliating for the anti-Islam movie and will continue its onslaught until the film is taken off the Web.

by Dara Kerr | September 25, 2012 9:23 PM PDT

Follow

Wells Fargo is the most recent mega-bank to be hit by a distributed denial-of-service attack. According to the Wall Street Journal, roughly 220 customers filed complaints of outages on its Web site today saying they had problems logging on.

"The amount of bandwidth that is flooding the websites is very large, much larger than in other attacks, and in a sense unprecedented," chief executive of private security firm CrowdStrike Dmitri Alperovitch told the Wall Street Journal.

ARBOR NETWORKS

Triple Crown Attack – Multi-vector on a New Level

- Three new tools being used
  - Tool.Brobot, Tool.Kamikaze and Tool.Amos
- Multiple concurrent attack vectors
  - GET and POST app layer attacks on HTTP and HTTPS
  - DNS query app layer attack
  - TCP SYN floods
  - Floods on UDP, TCP, ICMP and other IP protocols
- Unique characteristics of the attacks
  - Use of Shell booters (infected web servers) with high upstream b/w
  - Very high packet per second rates per individual source
  - Large bandwidth attack on multiple companies simultaneously

Lessons Learned

Enterprise

- Firewalls/IPS truly don't offer any protection
  - All companies attacked have these devices
- Carrier/MSSPs coverage has limits
  - Resource strain when customers get attacked simultaneously
  - Slower to upgrade to the latest releases/protections
- Need to deploy DDoS security in multiple layers
  - On premise for control and speed
  - Multiple upstream options

MSSPs

- Capacity models need to be re-evaluated as larger multi-vector multi-customer attacks have become a reality
- Increase speed of new technology adoption

ARBOR NETWORKS

Thank You

Julio Arruda
jarruda@arbor.net