AN INTRODUCTION TO DDOS ATTACK

Khaled Fadda

Consulting Engineer , Arbor Networks – Middle East

kfadda@arbor.net

MENOG 16, Istanbul / Turkey

DDOS BACKGROUND

- What is a DDoS “ Distributed Denial Of Service” attack ?
  - An attempt to consume finite resources, exploit weaknesses in software design or implementations , or exploit lac of infrastructure .
  - Target the availability and utility of computing and network resources.
  - DDoS attacks effect availability! No Availability , no applications/services/data/internet ! NO revenue!
  - Attacks are almost always distributed for more significant effect.

AVAILABILITY IS HARD !

- **The Primary goal for DDoS defense is maintaining availability in the face of the attack.**
- Maintaining availability in the face of attack requires a combinations of skills, architecture, operational agility, analytical capabilities and mitigation capabilities.
- In Practice, most organizations never take availability into account when designing /speccing /building/deploying/testing/online apps/services/ properties.
- In Practice, most organizations never make the logical connection between maintaining availability and business continuity.
- In practice, most organizations never stress-test their apps serves stacks in order to determine scalability/resiliency shortcomings and proceed to fix them.
- In practice, most organizations do not have plans for DDoS mitigation – or if they have a plan , they never rehearse it!

DDOS ATTACKS

- DDoS attacks can consist of just about anything
  - Large quantities of raw traffic designed to overwhelm a resource or infrastructure
  - Application specific traffic designed to overwhelm a particular service – sometimes stealthy in nature
  - Traffic formatted in such a way to disrupt a host from normal processing
  - Traffic reflected and/or amplified through legitimate hosts
  - Traffic from compromised sources or from spoofed IP addresses
  - Pulsed attacks – start/stop attacks

- DDoS attacks can be broken out by category

DDOS ATTACK CATEGORIES

Volumetric, Brute Force attacks

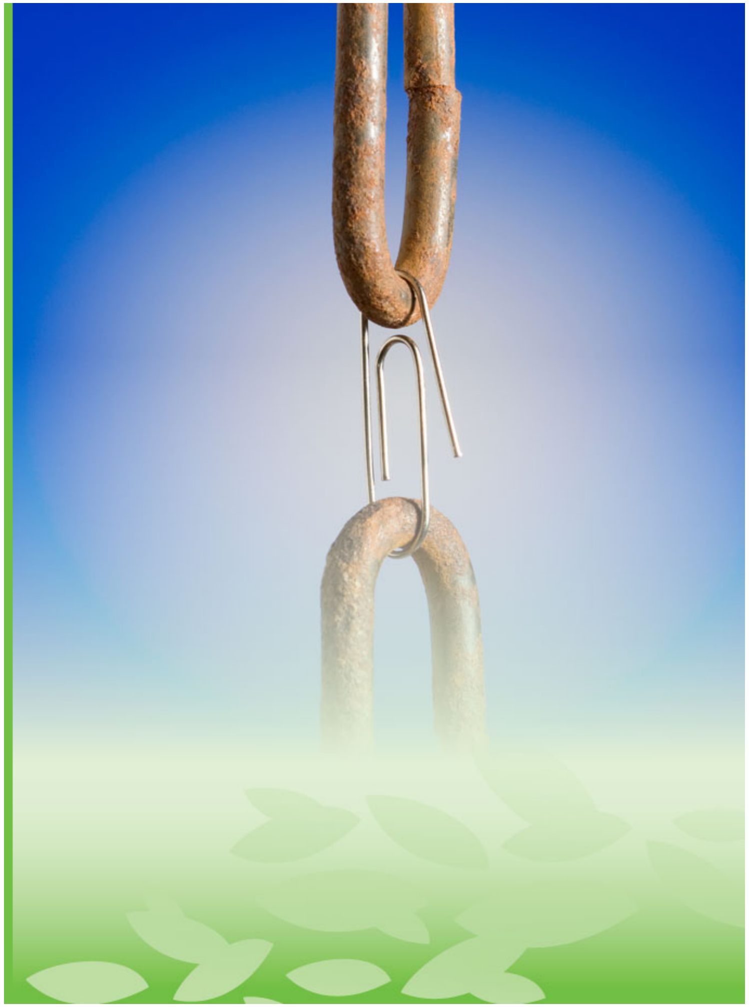
- **Traffic Floods**
  - Exhaust resources by creating high bps or pps volumes
  - Overwhelm the infrastructure – links, routers, switches, servers

Layer 4-7, Smart attacks

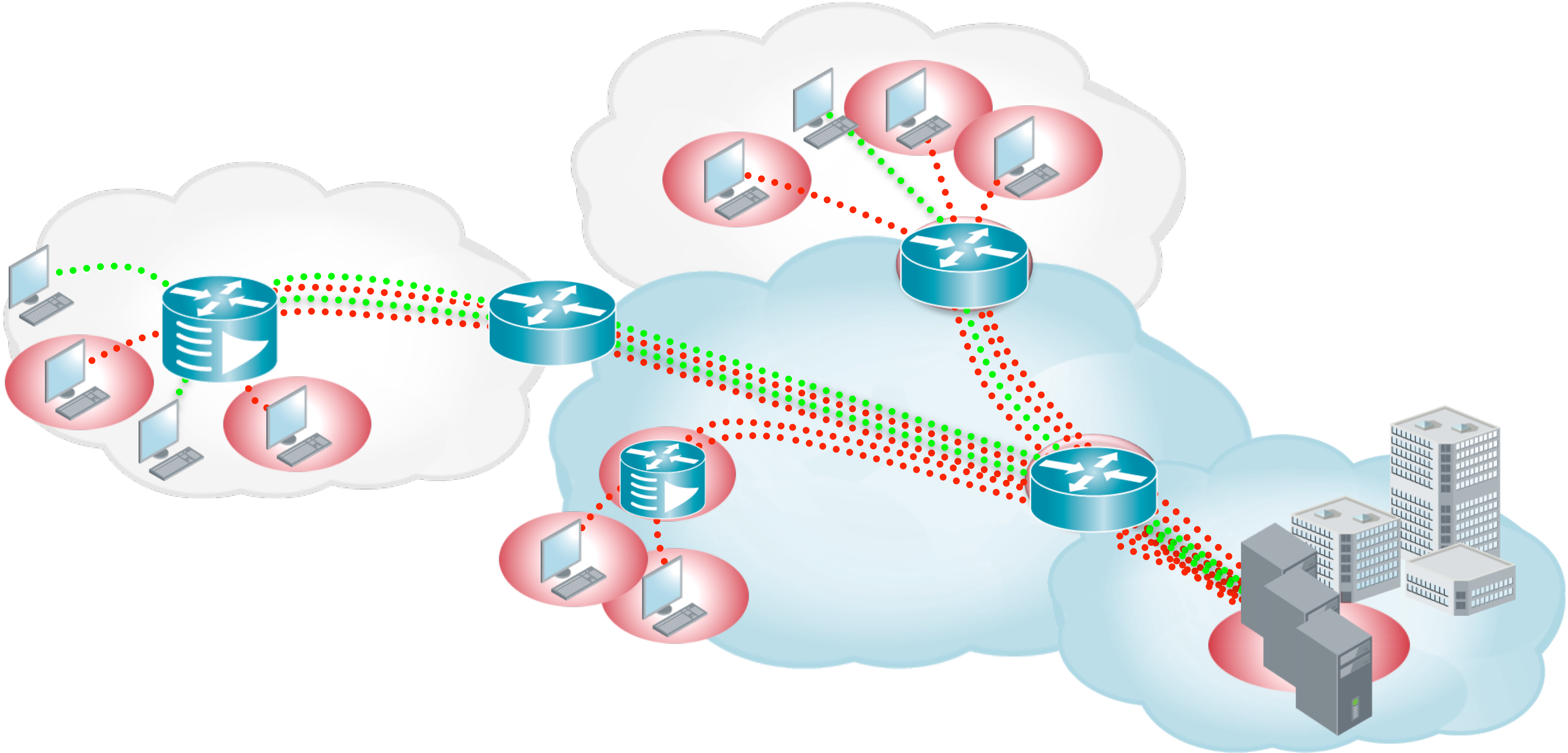
- **TCP resource exhaustion**
  - Exhaust resources in servers, load balancers, firewalls or routers
- **Application Layer**
  - Take out specific services or applications

THE DDOS ATTACK SURFACE

- Any part of your network or services that is vulnerable to an attack
  - Network Interfaces
  - Infrastructure
  - Firewall/IPS
  - Servers
  - Protocols
  - Applications
  - Databases
- Attackers will find the weakness



How a DDoS Attack works?

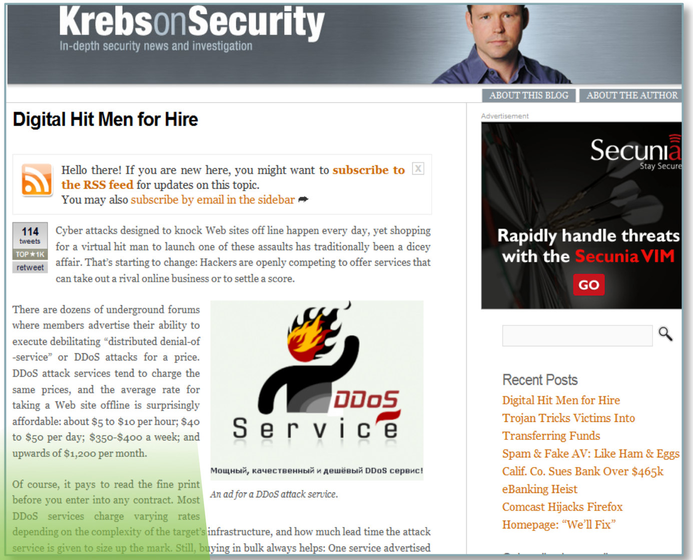


During a **Distributed Denial of Service (DDoS) attack**, [compromised] hosts or **bots** coming from distributed sources overwhelm the target with [il]legitimate traffic so that the servers cannot respond to legitimate clients.

→ **Critical services are <u>no longer available!</u>**

BOTS AND BOTNETS

- Botnets can have 100,000s of Bots
- Why use Bots to attack a destination?
    - Cheap
    - Practically untraceable
    - No one tries to clean up the bots



KrebsonSecurity
In-depth security news and investigation

Digital Hit Men for Hire

Hello there! If you are new here, you might want to **subscribe to the RSS feed** for updates on this topic.
You may also subscribe by email in the sidebar ➡

Cyber attacks designed to knock Web sites off line happen every day, yet shopping for a virtual hit man to launch one of these assaults has traditionally been a dicey affair. That's starting to change: Hackers are openly competing to offer services that can take out a rival online business or to settle a score.

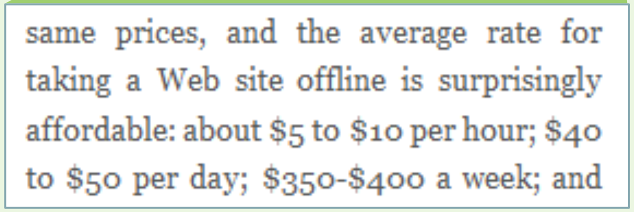
There are dozens of underground forums where members advertise their ability to execute debilitating "distributed denial-of-service" or DDoS attacks for a price. DDoS attack services tend to charge the same prices, and the average rate for taking a Web site offline is surprisingly affordable: about $5 to $10 per hour; $40 to $50 per day; $350-$400 a week; and upwards of $1,200 per month.

An ad for a DDoS attack service.

Of course, it pays to read the fine print before you enter into any contract. Most DDoS services charge varying rates depending on the complexity of the target's infrastructure, and how much lead time the attack service is given to size up the mark. Still, buying in bulk always helps: One service advertised

Recent Posts

Digital Hit Men for Hire
Trojan Tricks Victims Into Transferring Funds
Spam & Fake AV: Like Ham & Eggs
Calif. Co. Sues Bank Over $465k eBanking Heist
Comcast Hijacks Firefox Homepage: "We'll Fix"

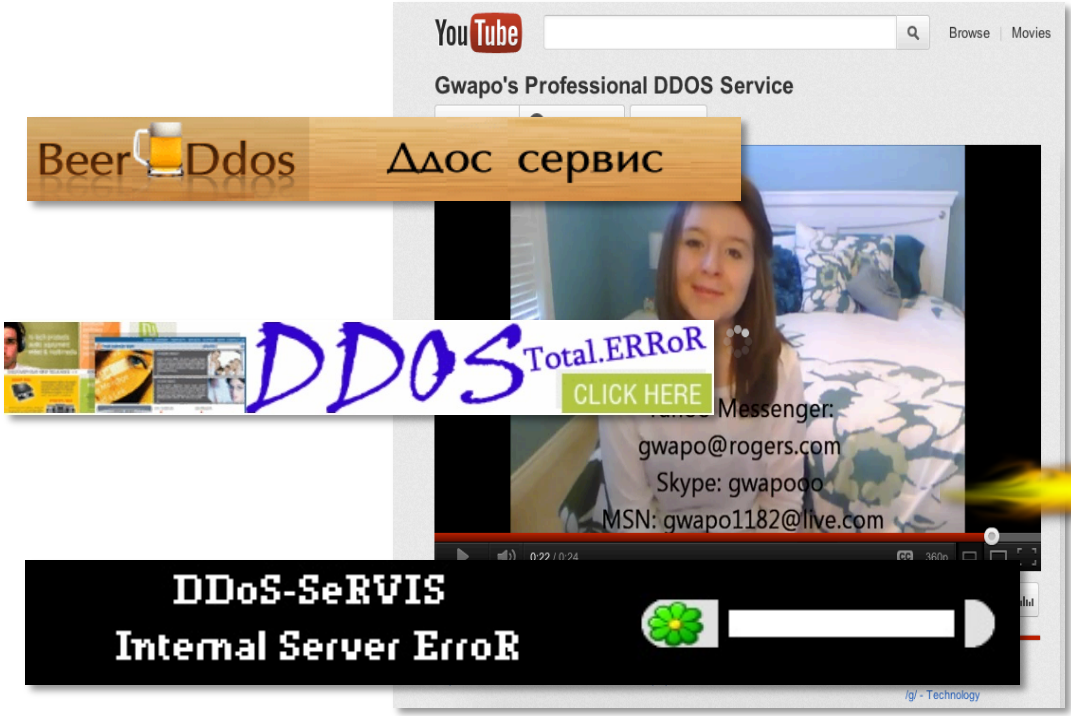


same prices, and the average rate for taking a Web site offline is surprisingly affordable: about $5 to $10 per hour; $40 to $50 per day; $350-$400 a week; and

Cost of a botnet to take a website off-line is as little as **$50 per day**

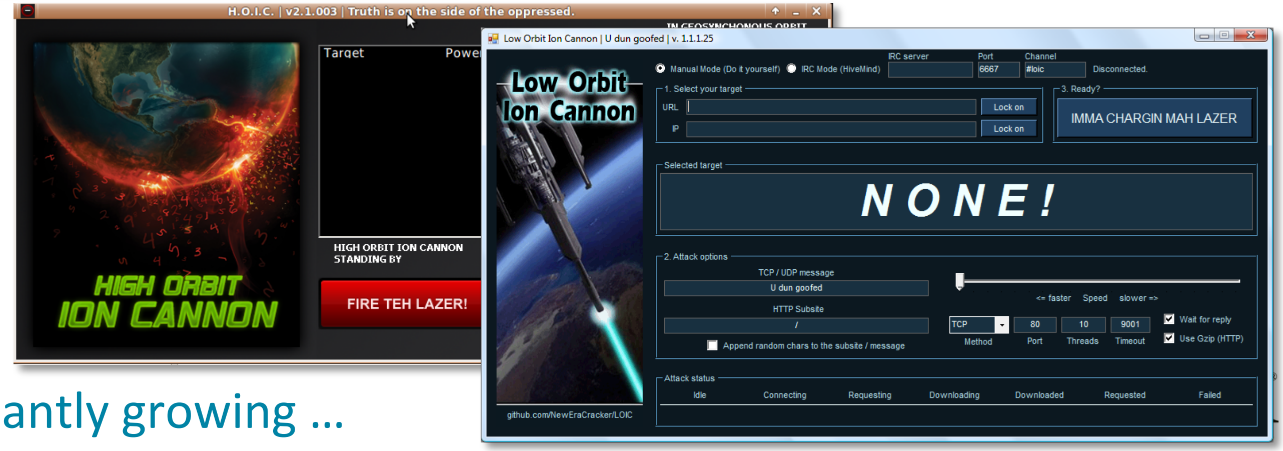
DDoS – “Services” & Tools

Commercial Tools & „Services“:



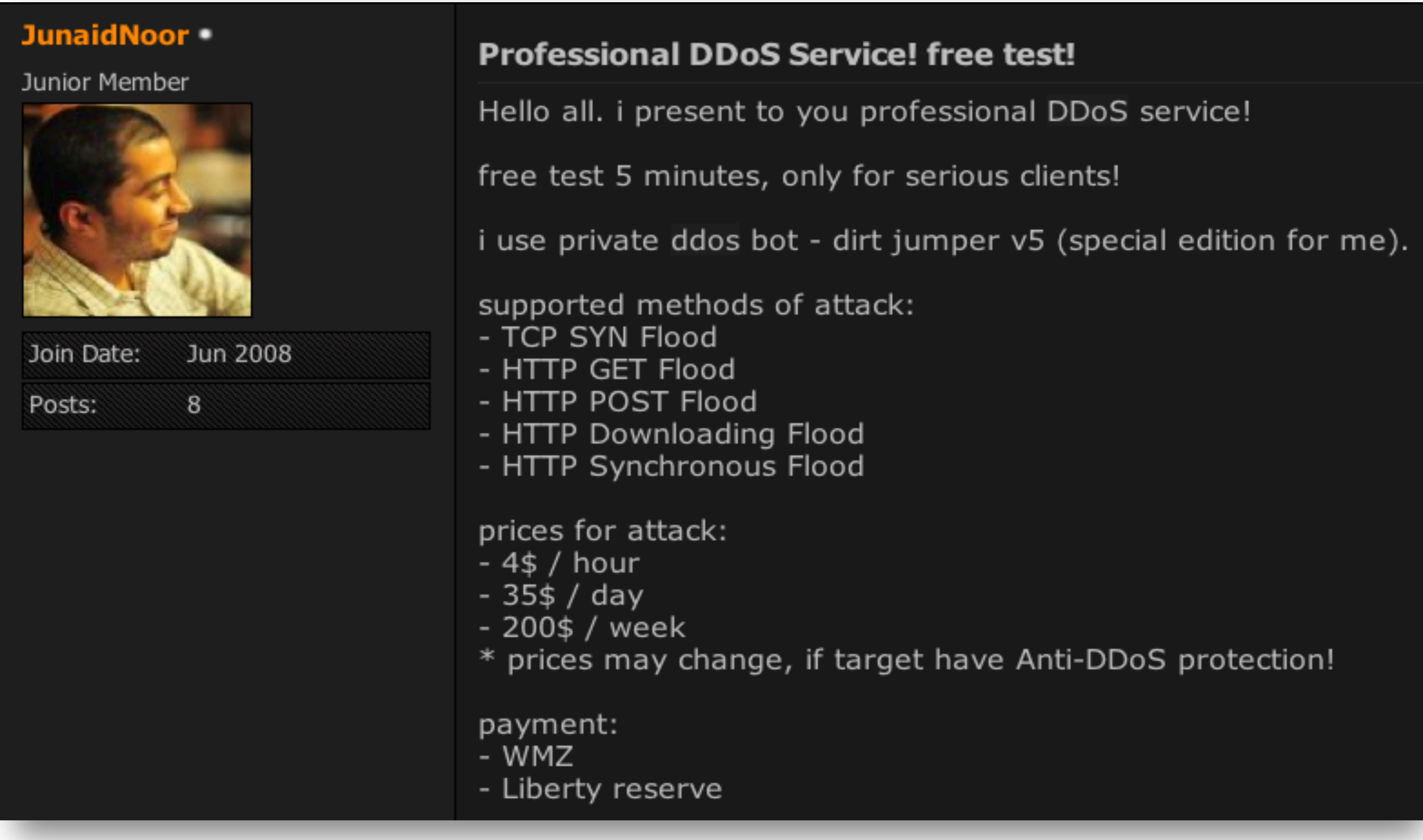
http,
icmp (ping),
syn,
udp.
Optima
DARKNESS X
Powerful DDoS Bot with premim admin-panel "Optima"
[From Russia with love]
4 types of DDoS Attacks/ Additional modules / 7 packages / Amazing Support
2009-2011. SW_Team
500 Internal
DDoS
Service
>>Выключим сайт конкурента или недруга<<
Работаем с HTTPS

New in 201x:
Voluntary „BotNet“



… many variations … constantly growing …

Commercial DDoS Services



JunaidNoor

Junior Member

Join Date: Jun 2008

Posts: 8

Professional DDoS Service! free test!

Hello all. i present to you professional DDoS service!

free test 5 minutes, only for serious clients!

i use private ddos bot - dirt jumper v5 (special edition for me).

supported methods of attack:
- TCP SYN Flood
- HTTP GET Flood
- HTTP POST Flood
- HTTP Downloading Flood
- HTTP Synchronous Flood

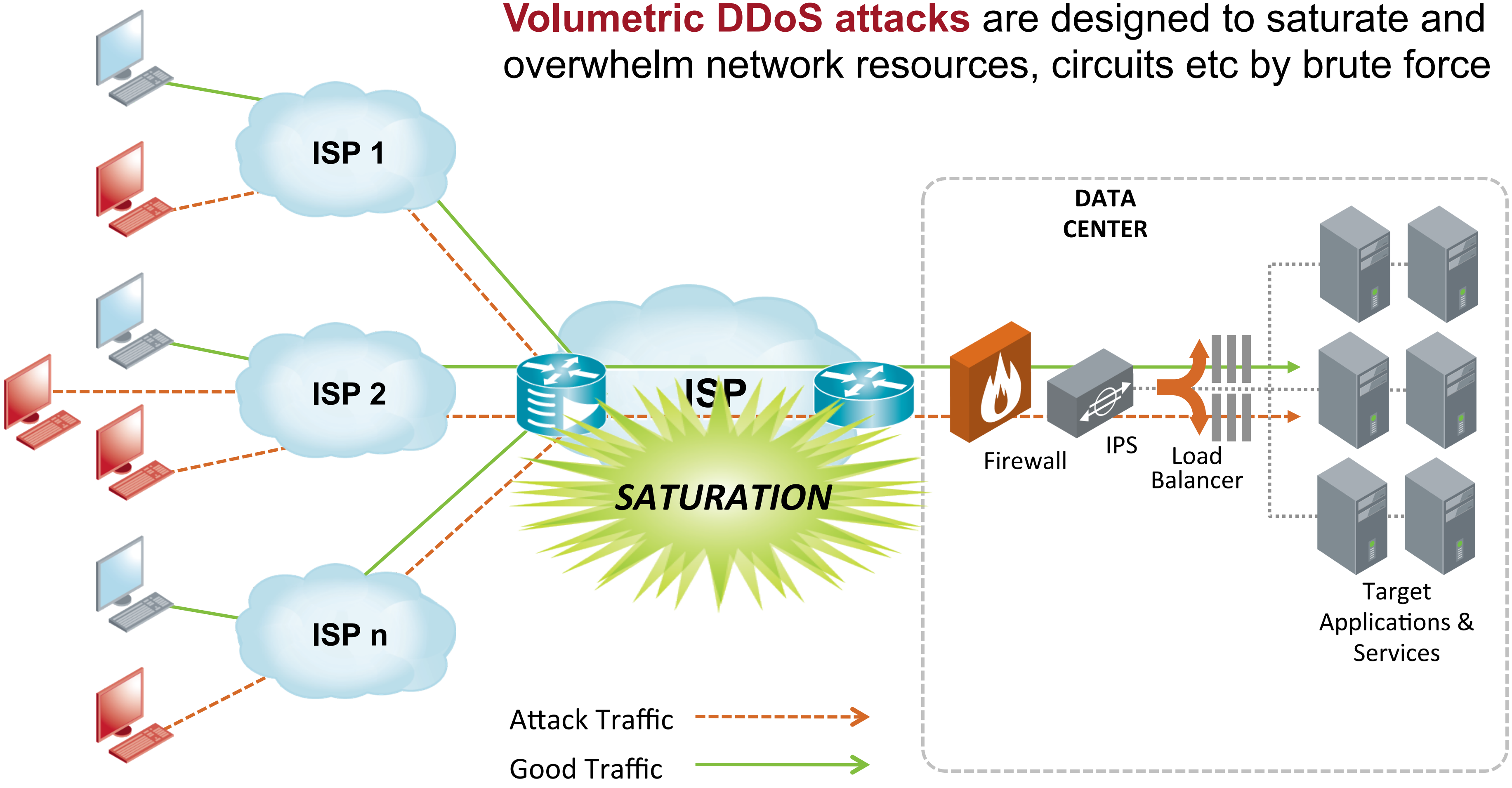
prices for attack:
- 4$ / hour
- 35$ / day
- 200$ / week

* prices may change, if target have Anti-DDoS protection!

payment:
- WMZ
- Liberty reserve

DDoS Attacks: Volumetric

Volumetric DDoS attacks are designed to saturate and overwhelm network resources, circuits etc by brute force



HIGH BANDWIDTH VOLUMETRIC DDOS

Description

- Large volume of traffic in bps and/or pps.
- Traffic could be spoofed or not spoofed.

Affect on Network

- Network links become saturated.
- Software-based routers, switches, firewalls, ISPs get overwhelmed.

Affect on Services

- Legitimate users can't get to services.

Common Names

- Packet flood, UDP flood, TCP flood

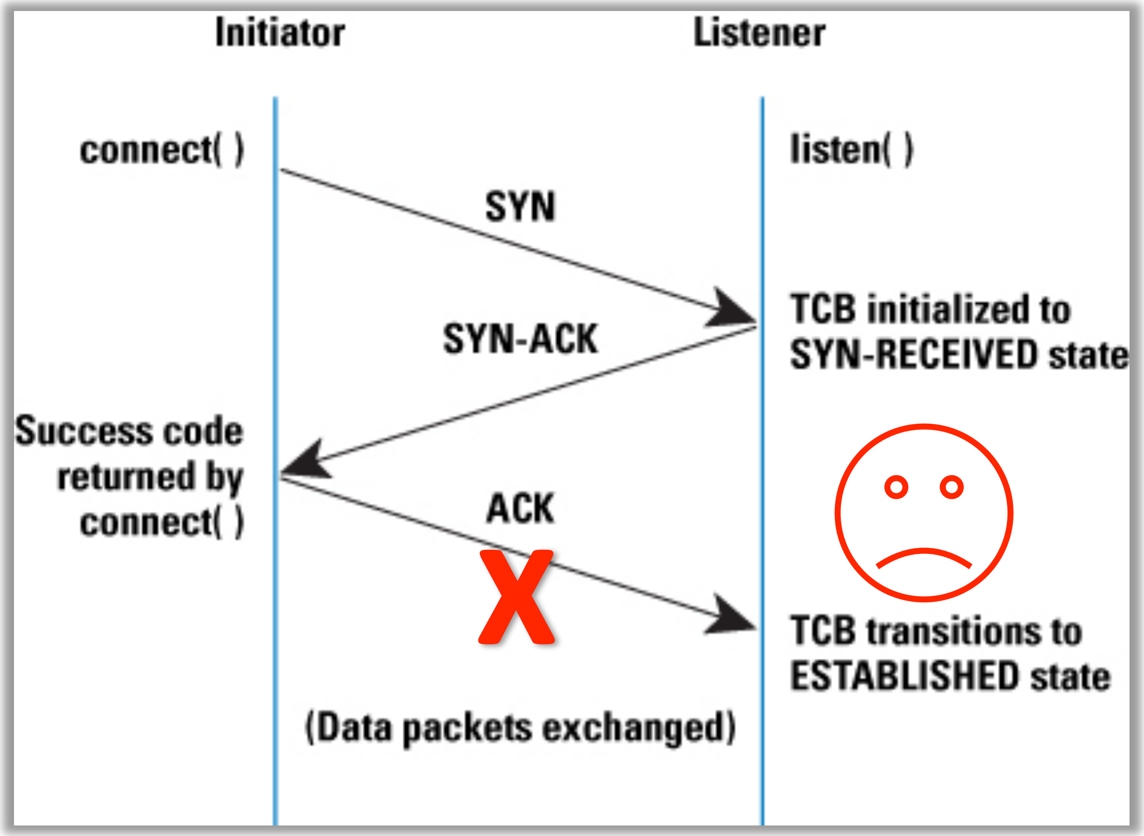
UDP Flood Attacks

- UDP is stateless, making it a common tool for flood attacks
  - Generation of UDP packets is easy
  - Stateless implies spoofing source IP addresses is possible
  - BPS and PPS: packet sizes may range from 60 to 1500 bytes
    - High volume of small packets can cause forwarding issues for routers and firewalls and other inline devices
    - 1Mpps @ 60bytes = 458Mbps
    - 1Mpps @ 1400bytes = 10Gbps
- UDP Floods do not generally impact services (unless DNS) but do impact the infrastructure causing collateral damage
  - UDP Floods can cause jitter and latency, impacting other services like VoIP

SYN Flood Attacks

- SYN flood attacks attempt to exhaust the server side resources for TCP connections
- Source(s) continuously send packets with just the SYN bit set
- Victim (Server) must open a connection and send a SYN-ACK back to the source
- Connection is kept open
  - Source ACK’s and then data is exchanged
  - Source terminates connection
  - Server times out the connection
- SYN packets are typically small in size

TCP Stack Attack – Syn Flood Attack


Initiator
Listener
connect( )
listen( )
SYN
TCB initialized to SYN-RECEIVED state
SYN-ACK
Success code returned by connect( )
ACK
X
TCB transitions to ESTABLISHED state
(Data packets exchanged)

Reflection Attacks

Description

- Attackers spoof IP address of victim as source and send queries to open proxies or resolvers that then send "answers" to the victim.
- Answers may be amplified if the response is bigger.

Affect on Network

- Network links become saturated.
- Software-based routers, switches, firewalls, ISPs get overwhelmed.

Affect on Services

- Legitimate users can't get to services.

Common Names

- DNS Reflection, DNSSec Amplification

Components of a Reflection/Amplification DDoS Attack

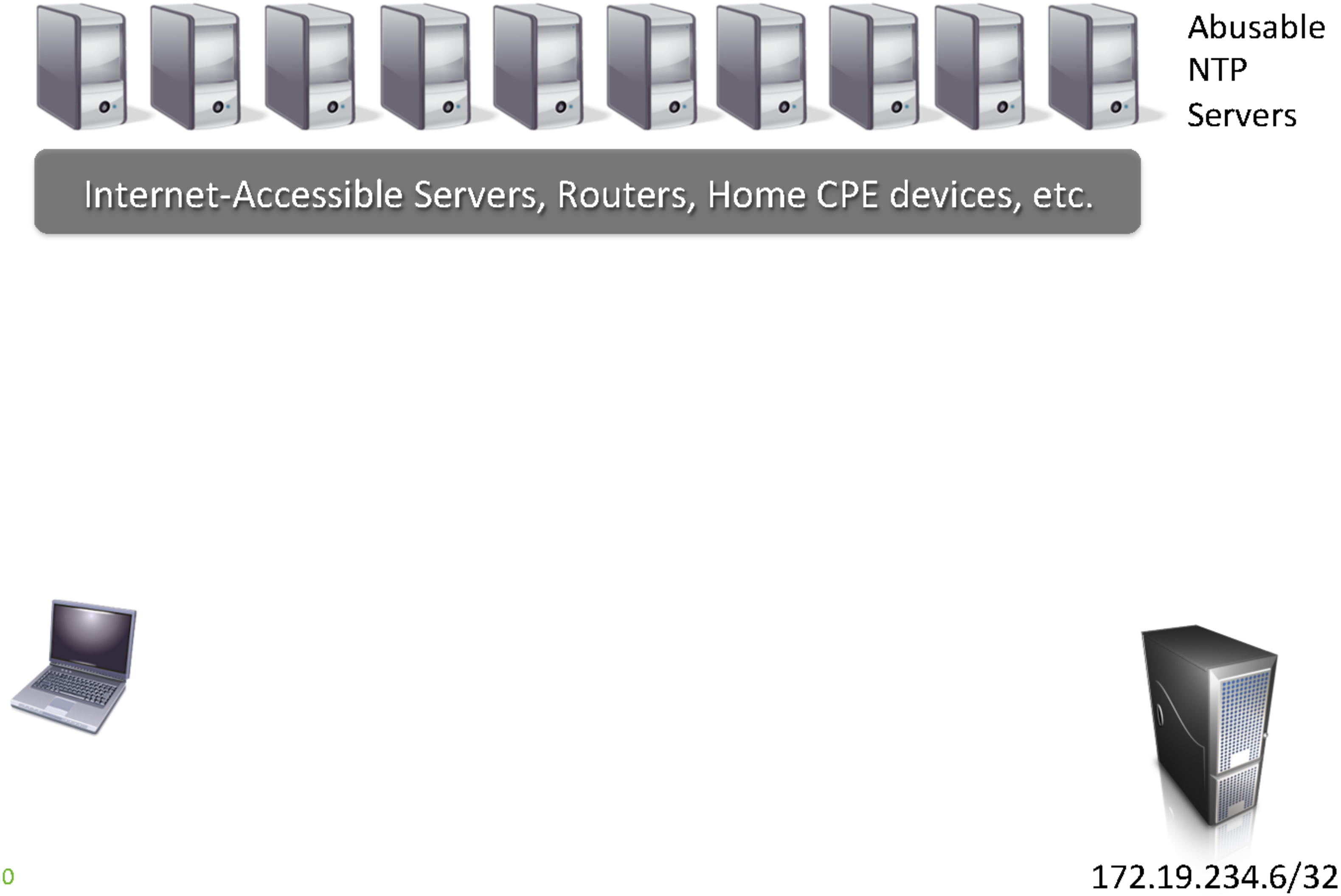
Amplification

- Attacker makes a relatively small request that generates a significantly-larger response/reply. This is true of most (not all) server responses.

Reflection

- Attacker sends spoofed requests to a large number of Internet connected devices, which reply to the requests. Using IP address spoofing, the 'source' address is set to the actual target of the attack, where all replies are sent. Many services can be exploited to act as reflectors.

NTP Reflection/Amplification Attack Methodology

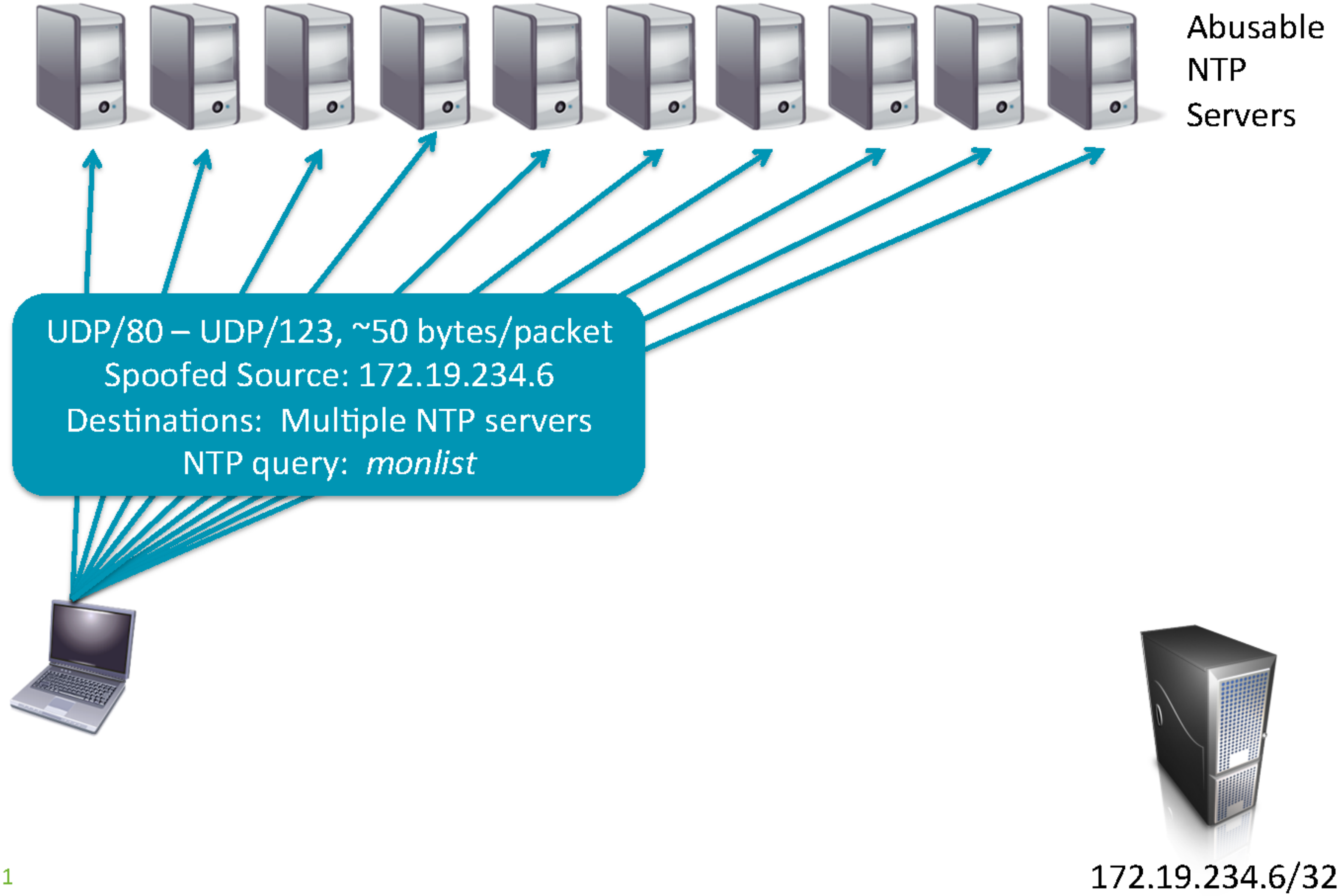


Abusable NTP Servers

Internet-Accessible Servers, Routers, Home CPE devices, etc.

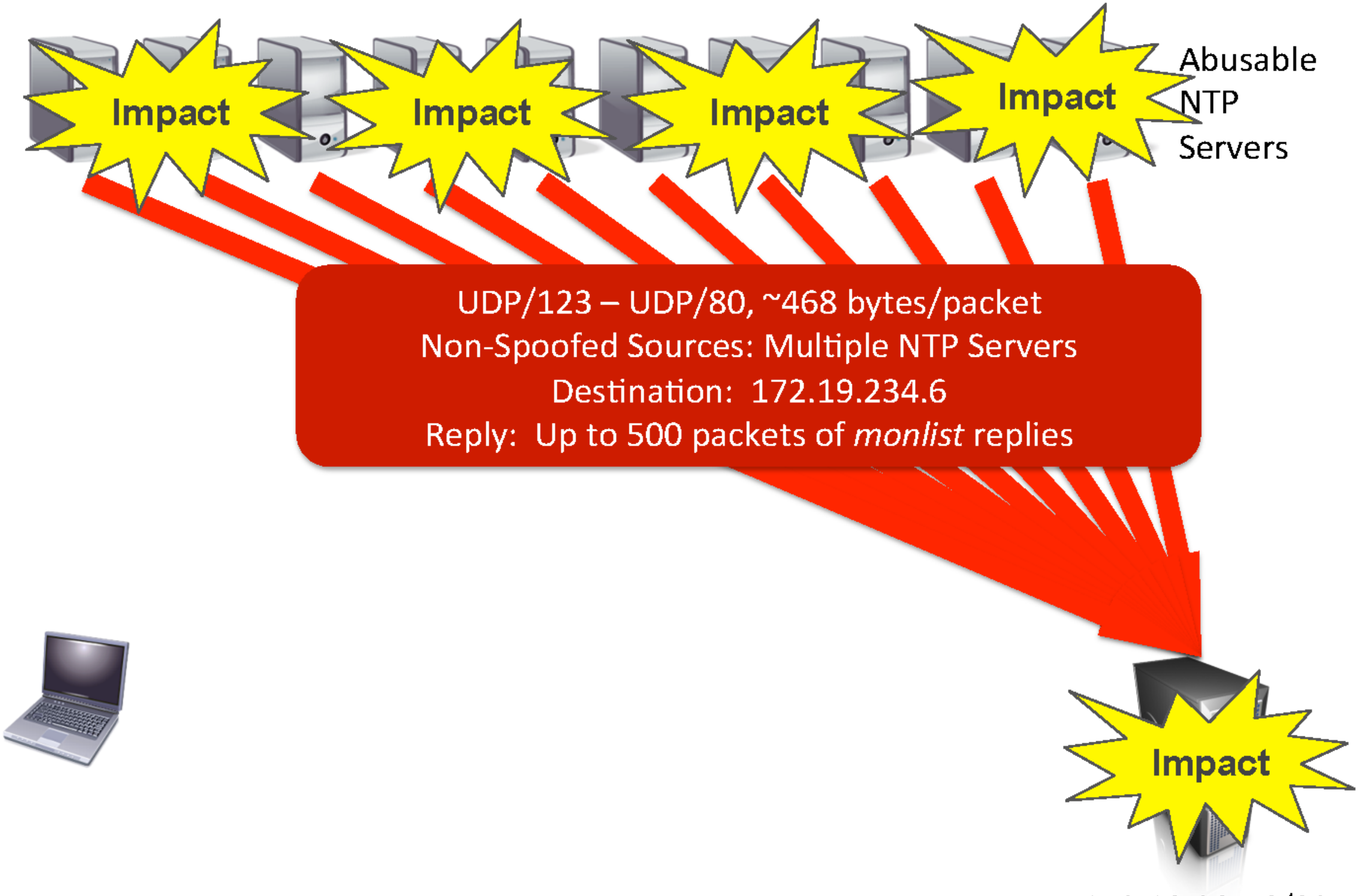
172.19.234.6/32

NTP Reflection/Amplification Attack Methodology



UDP/80 – UDP/123, ~50 bytes/packet
Spoofed Source: 172.19.234.6
Destinations: Multiple NTP servers
NTP query: *monlist*

NTP Reflection/Amplification Attack Methodology



UDP/123 – UDP/80, ~468 bytes/packet
Non-Spoofed Sources: Multiple NTP Servers
Destination: 172.19.234.6
Reply: Up to 500 packets of *monlist* replies

Five Common Reflection/Amplification Vectors

Abbreviation	Protocol	Ports	Amplification Factor	# Abusable Servers
CHARGEN	**Char**acter **Gen**eration Protocol	UDP / 19	18x/1000x	Tens of thousands (90K)
DNS	**D**omain **N**ame **S**ystem	UDP / 53	160x	Millions (27M)
NTP	**N**etwork **T**ime **P**rotocol	UDP / 123	1000x	Over One Hundred Thousand (119K)
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol	UDP / 161	880x	Millions (5M)
SSDP	Simple Service Discovery Protocol	UDP /1900	20x/83x	Millions (2M)

Protocols used for Reflection/Amplification

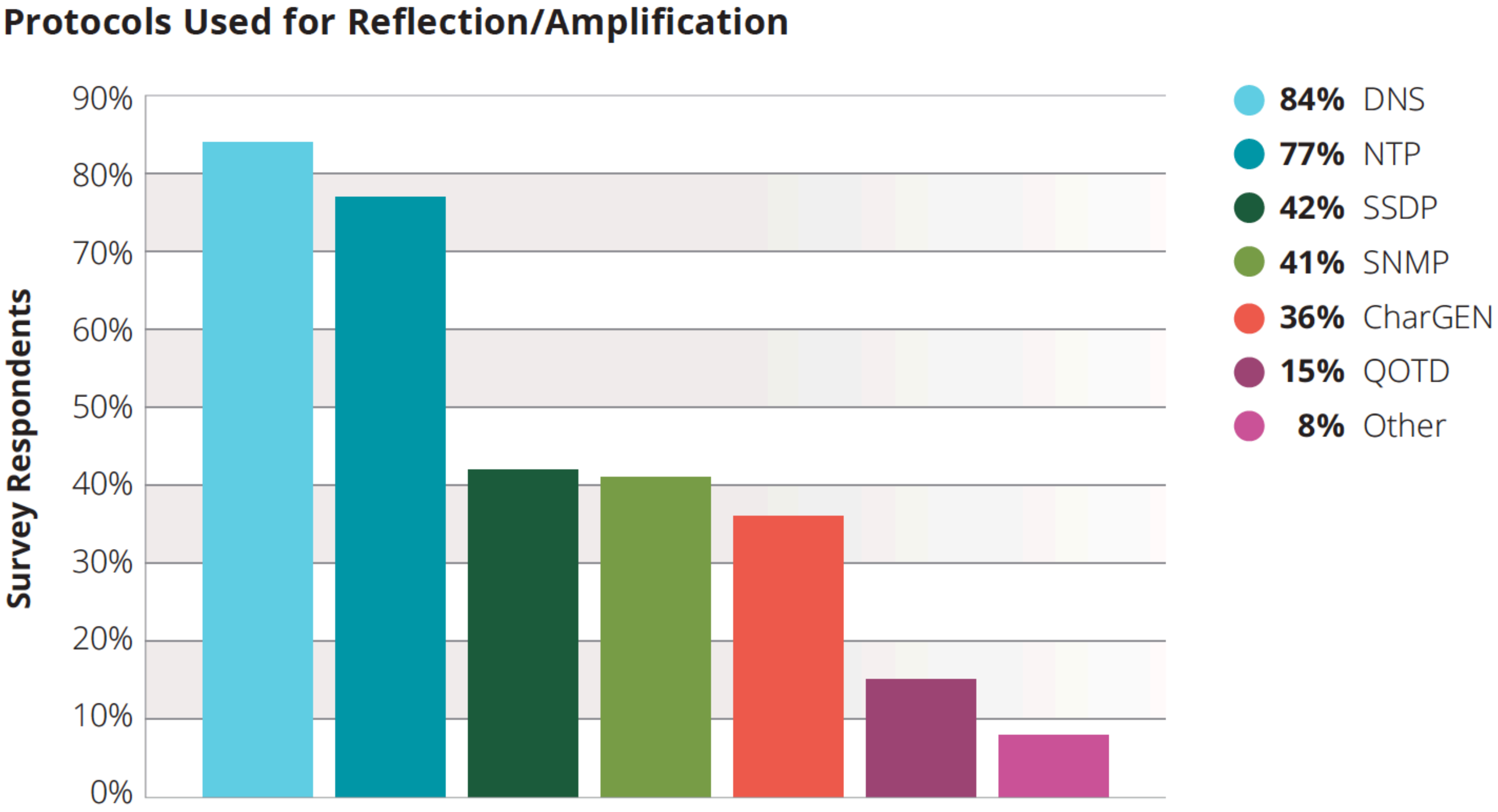
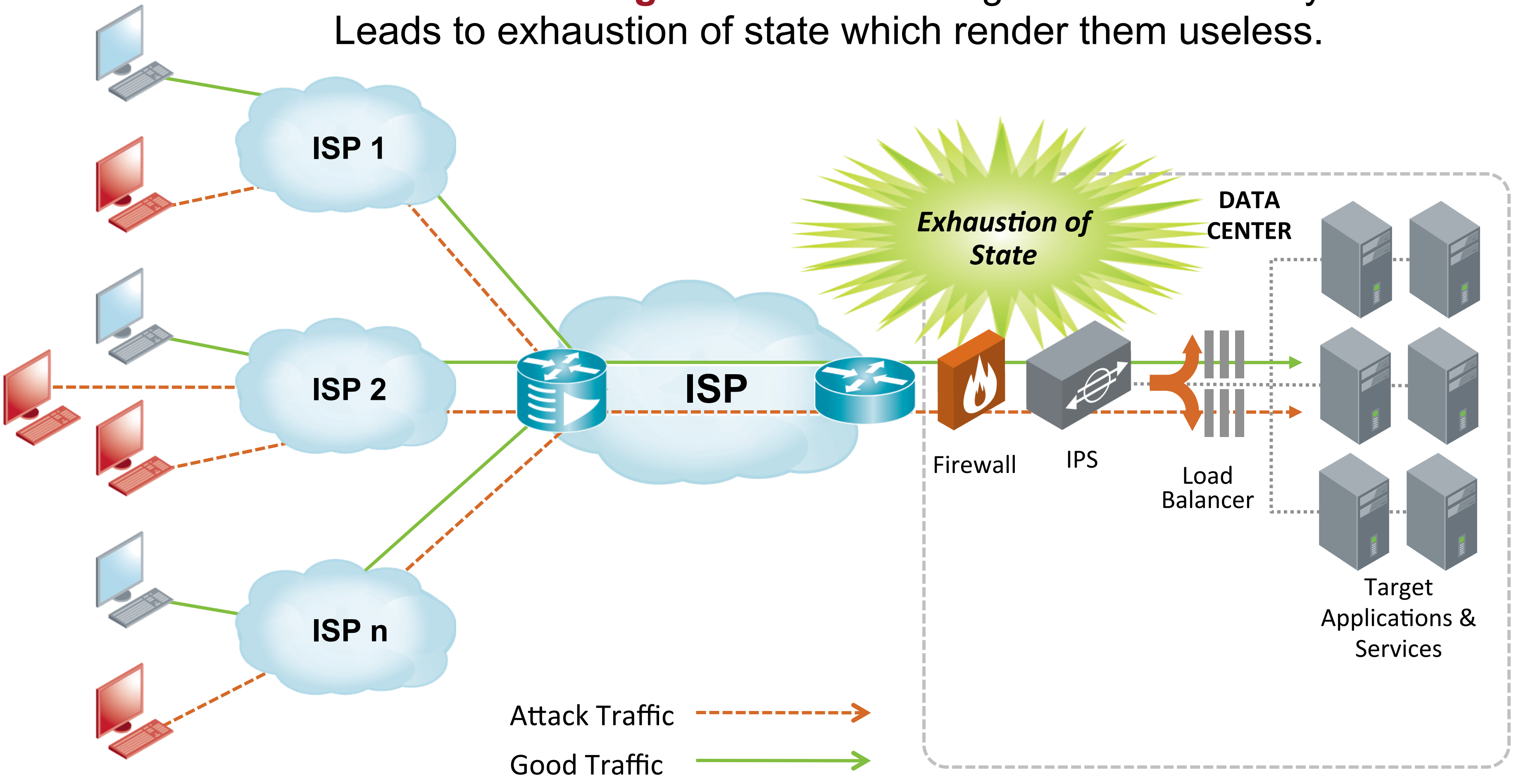


Figure 15 *Source: Arbor Networks, Inc.*

DDoS Attacks: State-Exhausting

State-Exhausting DDoS attacks target stateful security devices. Leads to exhaustion of state which render them useless.



Protocol Attacks

Description

- Attacks that exploit vulnerable parts of protocols such as TCP 3-way handshake. They are often crafted to overwhelm protocol state of devices

Affect on Network

- State table on servers, load balancers, IPS and firewalls fill up and they will no longer pass traffic

Affect on Services

- Legitimate users can't get to services.

Common Names

- SYN flood, RST flood, FIN flood

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.

Affect on Network

- Available connections to the service are exhausted. State tables of FW, IPS, load balancers could also get overwhelmed.

Affect on Services

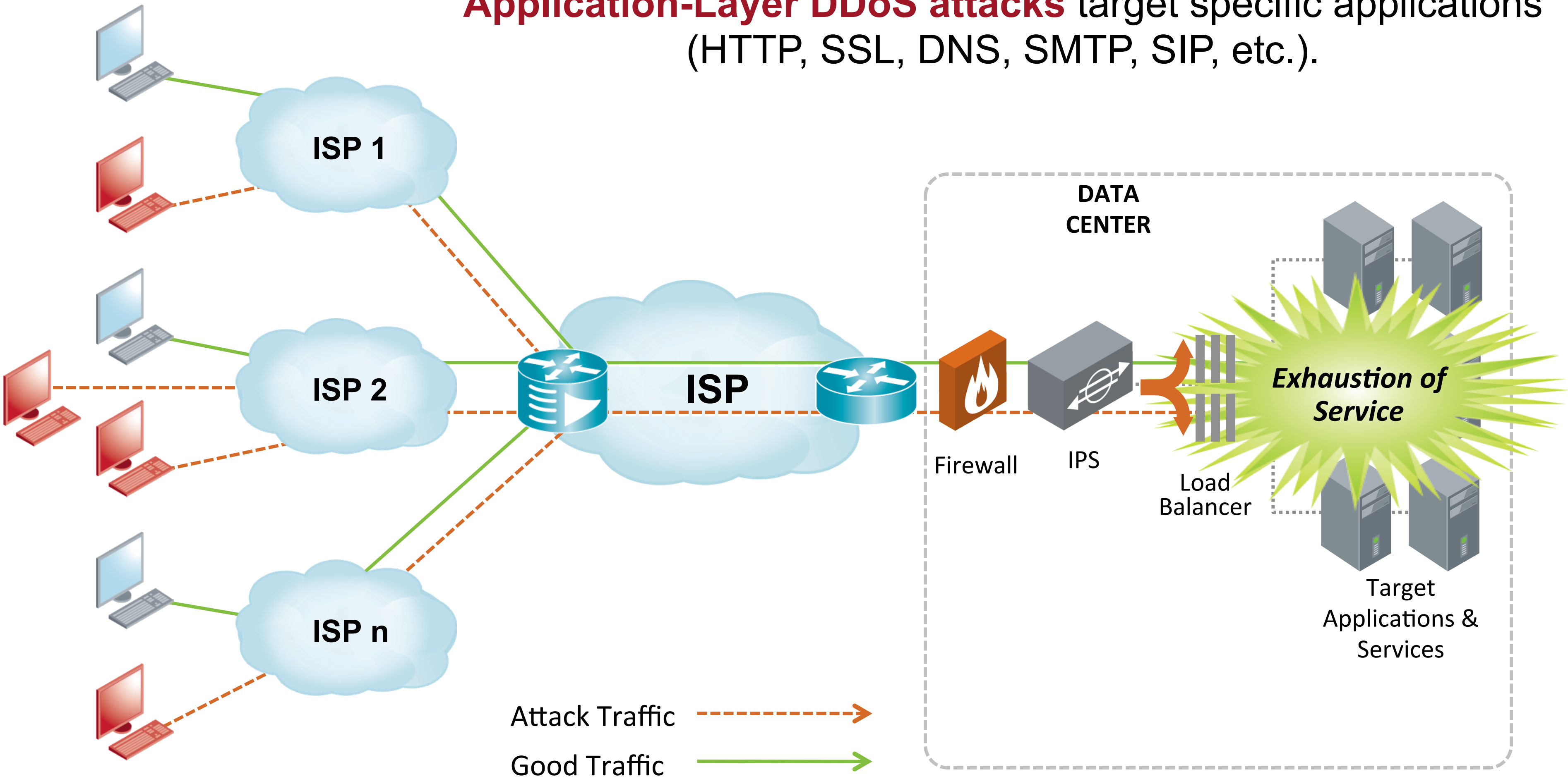
- Legitimate users can’t get to services.

Common Names

- Sockstress

DDoS Attacks: Application Layer

Application-Layer DDoS attacks target specific applications (HTTP, SSL, DNS, SMTP, SIP, etc.).



Application-Layer Attacks

Description

- Attacks that target a vulnerability at the application layer.
- Can range from application floods to slow stealthy attacks that target a particular weakness.

Affect on Network

- Limited network effect as the traffic rates can be very low.
- They sometimes cause congestion between services and storage databases.

Affect on Services

- Services become unresponsive or go down altogether.

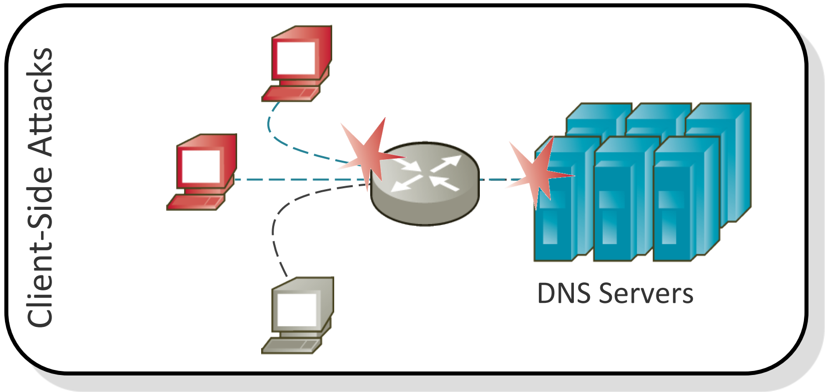
Common Names

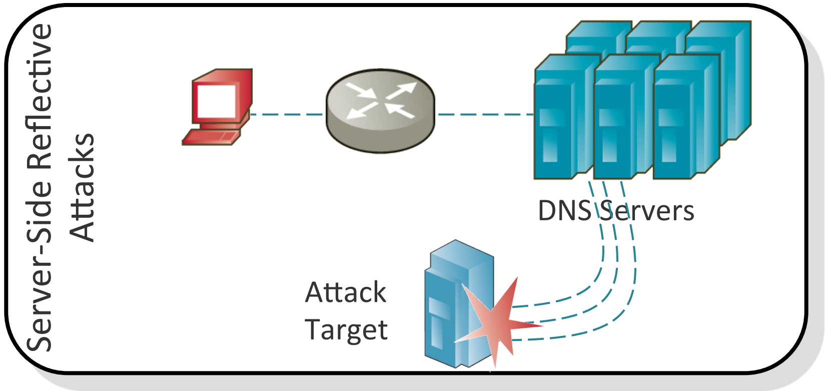
- URL floods, R U Dead Yet (RUDY), Slowloris, LOIC, HOIC, DNS dictionary attacks

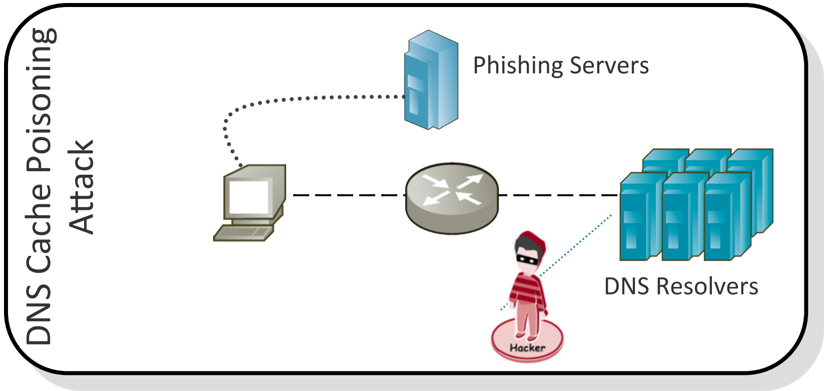
Application Attacks to Web Servers

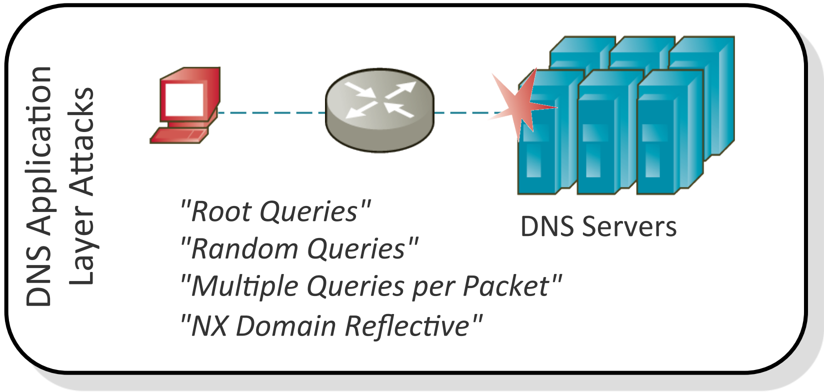
- Get Floods
  - Brute force use the server's processing capacity – typically done using a Botnet
  - Ex: Siege
- Slow GET
  - Creates TCP sessions that never close and hold server resources (TCP table space, process table, memory)
  - Ex: Slowloris
- Slow POST
  - Similar to Slow GET, focused on pages which have forms to be completed (can't be cached by CDNs)
  - Ex: RUDY

Common DNS Attacks









- Multiple threat vectors against DNS whose impacts include loss of service availability, reduced customer satisfaction, and hurt profitability

Targets of Application-layer attacks

Targets of Application-Layer Attacks

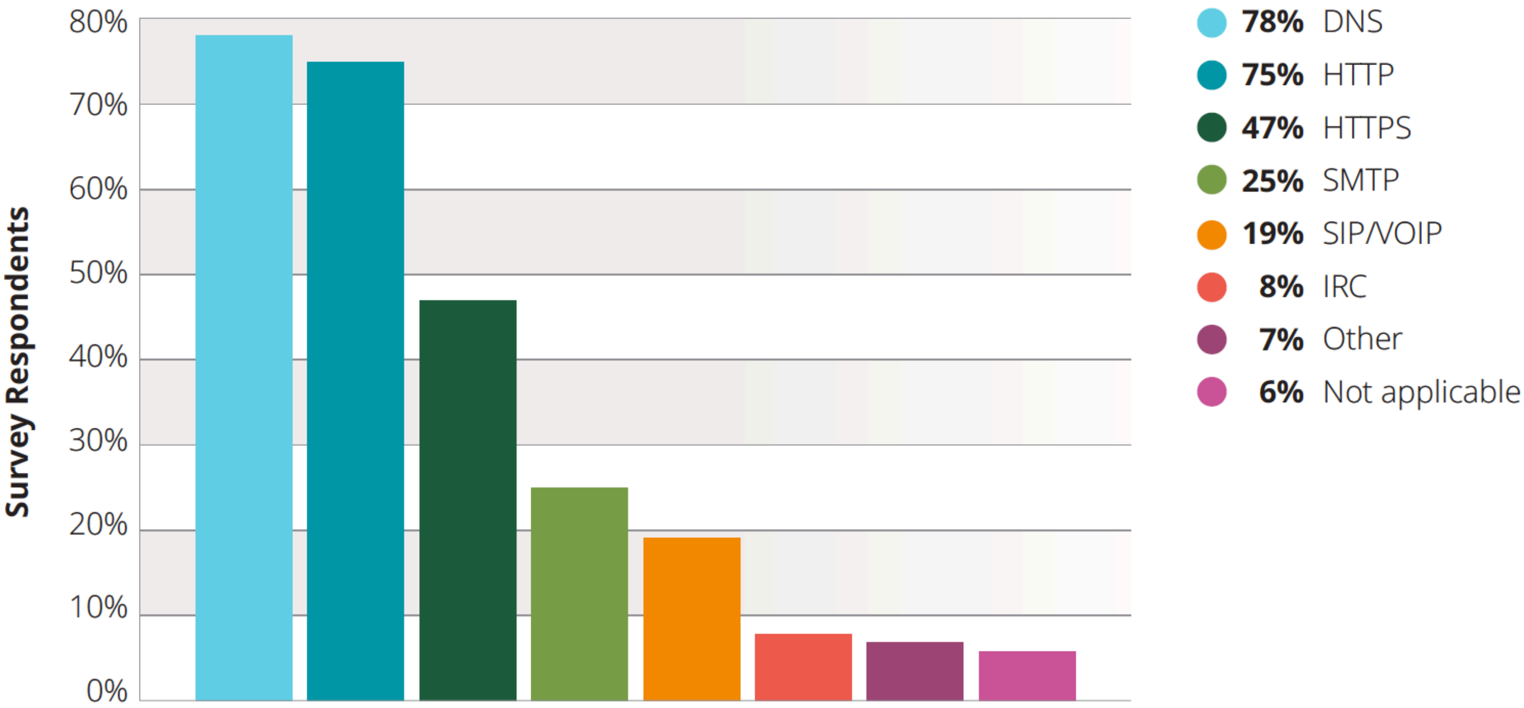


Figure 21 *Source: Arbor Networks, Inc.*

DDoS is an Exploding & Evolving Trend

More Attack Motivations

Geopolitical “Burma taken offline by DDOS attack”

Protests “Visa, PayPal, and MasterCard attacked”

Extortion “Techwatch weathers DDoS extortion attack”

+

Greater Availability of Botnets

Better Bots More infected PCs with faster connections

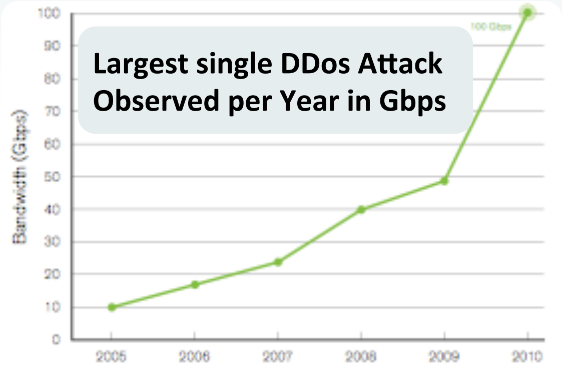
Easy Access Using web 2.0 tools to control botnets

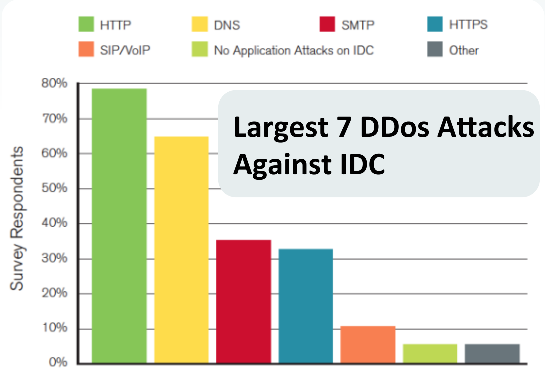
Commoditized Cloud-based botnets, cheaper

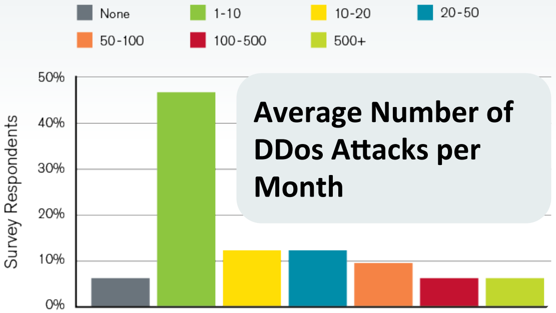
=

more attacks

Increased Volume	Increased Complexity	Increased Frequency
Largest **volumetric** DDoS has grown to 500+ Gbps in 2015	Over 25% of attacks are **application-based** DDoS mostly targeting HTTP, DNS, SMTP	>50% of data center operators experience >10 attacks per month

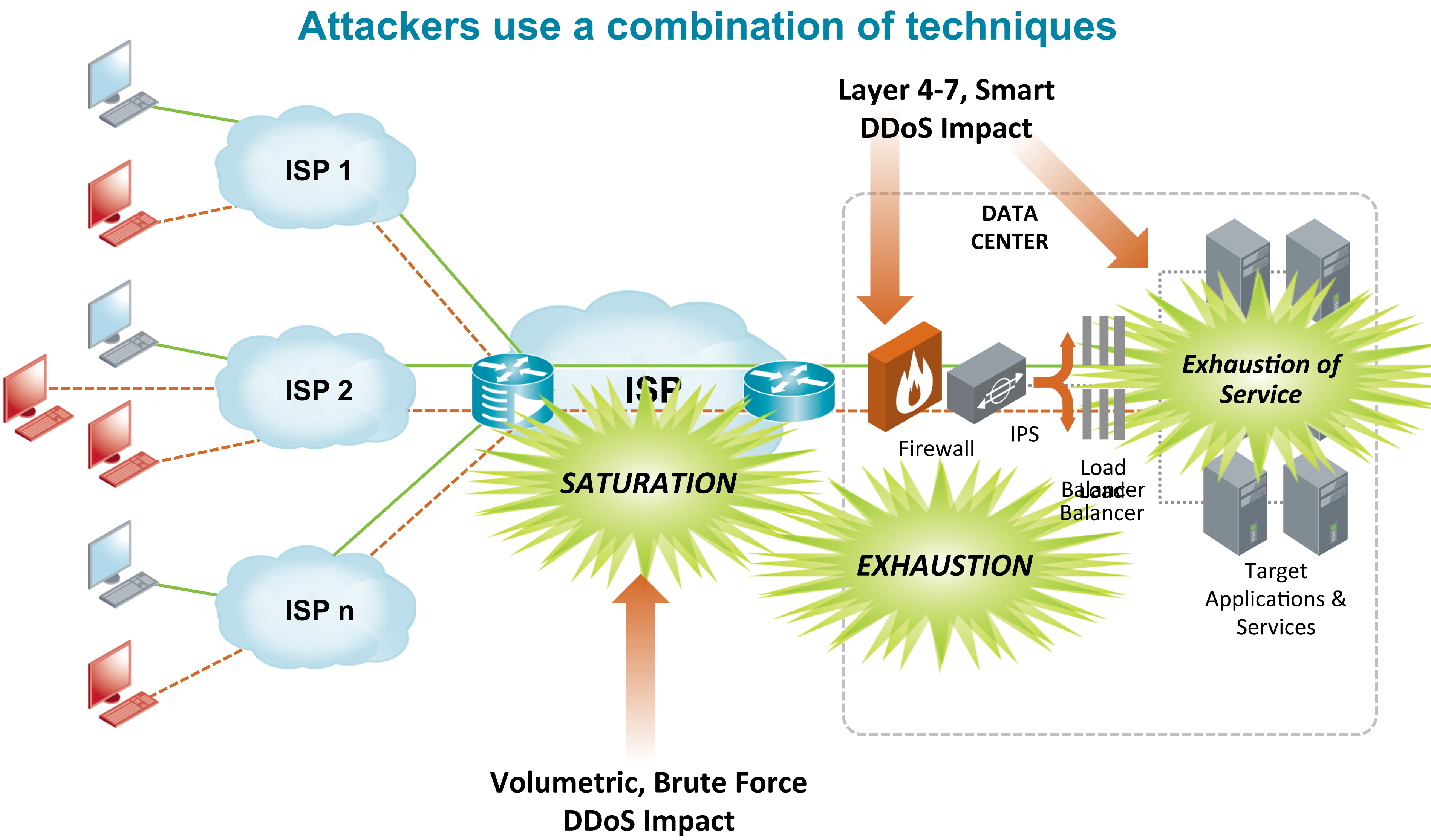

Largest single DDos Attack Observed per Year in Gbps


Largest 7 DDos Attacks Against IDC


Average Number of DDos Attacks per Month

ARBOR NETWORKS

The Evolving DDoS Threat



Substantial Growth in Largest Attacks

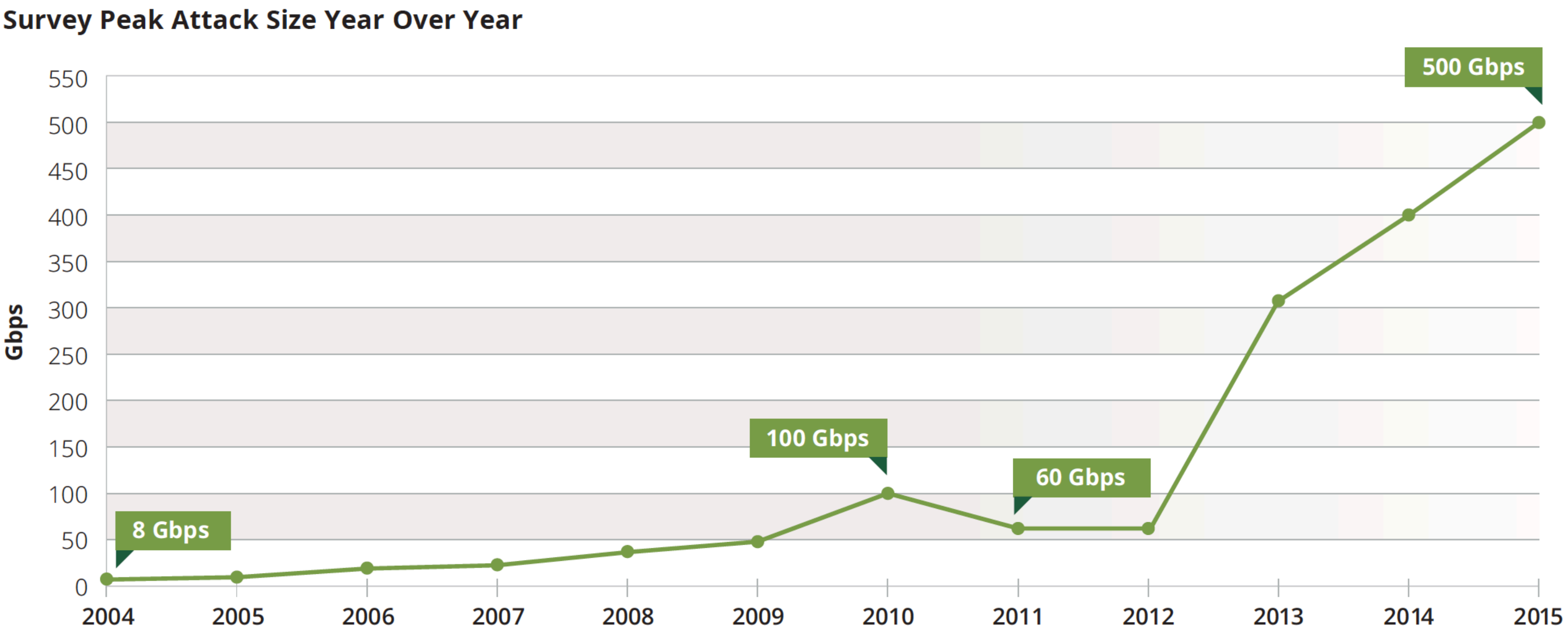
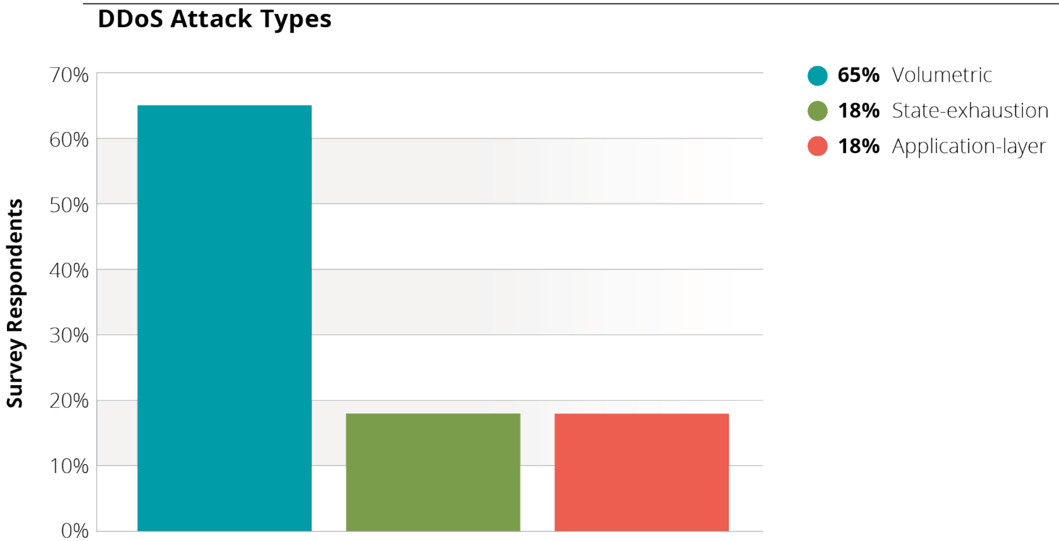


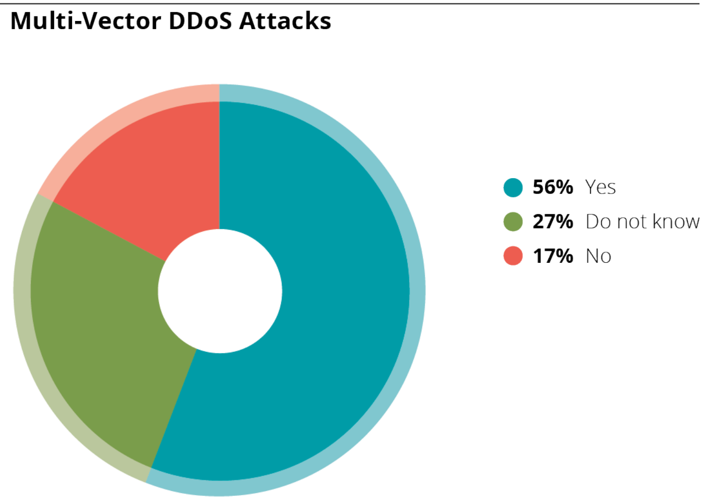
Figure 14 *Source: Arbor Networks, Inc.*

- Largest reported attacks ranged from 500 Gbps at the top end, through 450Gbps, 425Gbps and 337Gbps

DDoS – Complexity Increases



Source: Arbor Networks, Inc.



Source: Arbor Networks, Inc.

- Media focus on volumetric attacks, stealthy application-layer attacks haven’t gone away
  - 93% of respondents see application-layer attacks, up from 90% last year and 86% in 2013
- DNS is now top application-layer target, over-taking HTTP
  - Strong growth in respondents seeing attacks targeting SIP / VoIP services, up from 9% to 19%
- 56% see multi-vector attacks, up from 42% last year

Firewalls and Intrusion Protection/Detection Systems (IDS/IPS)

Firewalls are policy-enforcement devices – they can’t help with DDoS, and in most cases, the policies applied to the firewalls have been devised with no visibility into network traffic, so the firewall rules bear little relation to what should actually be permitted and denied.

IDS/’IPS’ are by definition always behind the attackers – in order to have a signature for something, you must have seen it before.

IDS/’IPS’ have proven to be totally ineffective at dealing with application-layer compromises, which is how most hosts are botted and used for DDoS, spam, corporate espionage, identity theft, theft of intellectual property, etc.

Firewalls & IDS/’IPS’ output reams of syslog which lacks context, and which nobody analyzes. It is almost impossible to relate this syslog output to network behaviors.

End-customers subscribe to traditional managed security services based on firewalls and IDS/’IPS’, and still get compromised.

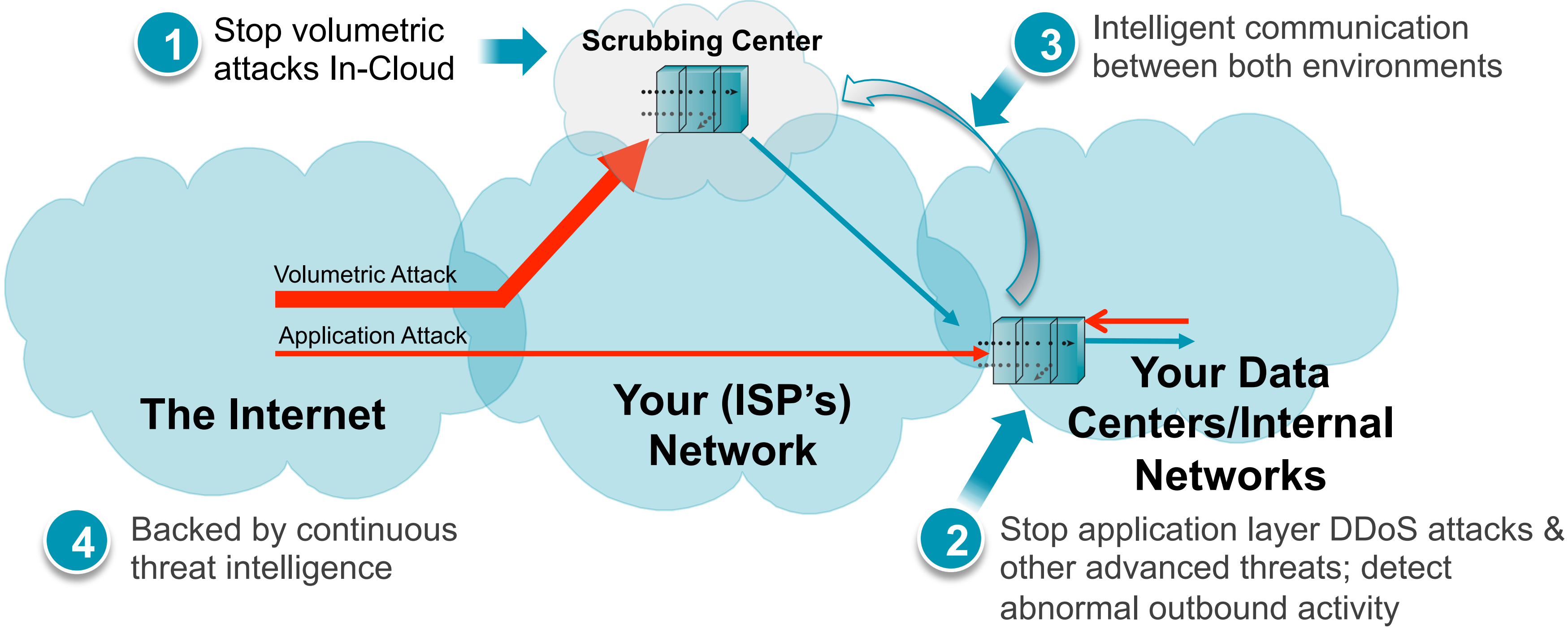
Firewall & IDS/’IPS’ deployments cause performance & usability problems, and don’t scale.

Reacting to a DDoS Attack

- ACL
- Black Hole Filtering (S/RTBH)
- BGP FlowSpec
- On-premise IDM solutions (DDoS solutions).
- Layered-DDoS Attack Surgical mitigation solution.

STOPPING DDoS ATTACKS

Layered DDoS Attack Protection



1 Stop volumetric attacks In-Cloud

3 Intelligent communication between both environments

Scrubbing Center

Volumetric Attack

Application Attack

The Internet

Your (ISP's) Network

Your Data Centers/Internal Networks

4 Backed by continuous threat intelligence

2 Stop application layer DDoS attacks & other advanced threats; detect abnormal outbound activity

Backed by Continuous Threat Intelligence

A Recommended Industry Best Practice:

FORRESTER® IDC FROST & SULLIVAN Infonetics RESEARCH Securosis ovum

THANK YOU

WWW.ARBORNETWORKS.COM