



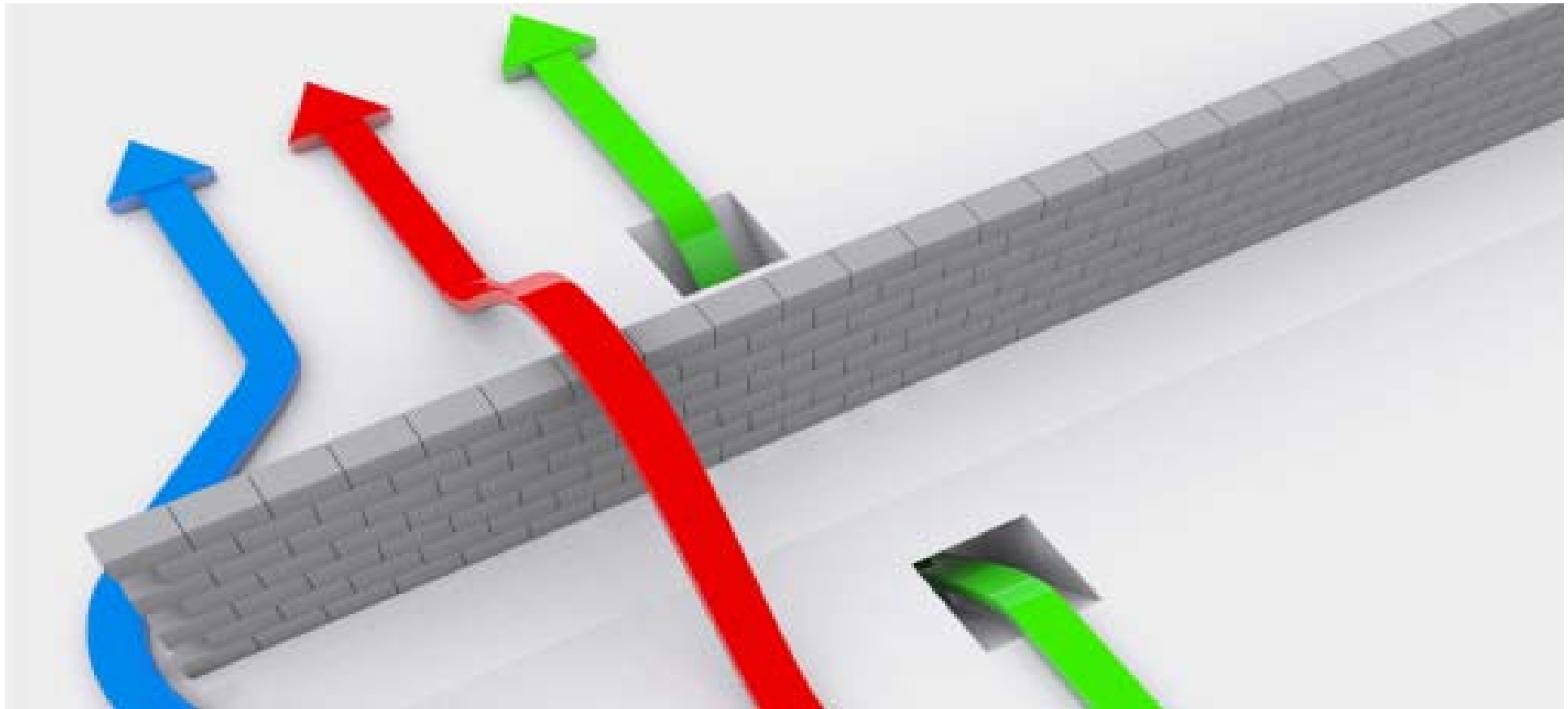
What is DDoS and the Mitigation Strategies

Frank Tse, Nexusguard

Agenda

- 1 What is DDoS
- 2 What does DDoS look like
- 3 Impact of DDoS
- 4 Who will be under risk of DDoS
- 5 DDoS attack types
- 6 Who is attacking
- 7 Why DDoS is so popular
- 8 Case study
- 9 DDoS solutions

About us



“Nexusguard is a provider of end-to-end, in-the-cloud, Internet Security Solutions.”

Recent DDoS Headlines

INTERNATIONAL BUSINESS TIMES
Anonymous Launches DDoS Attack On Sony
By Jesse Emspak | April 6, 2011 5:17 PM EDT

FINANCIAL TIMES
August 11, 2011 3:47 pm
Hong Kong exchange hacked again
By Enid Tsui in Hong Kong

dt DIGITAL TRENDS
aggregates your thoughts
LulzSec DDoS attacks disrupt CIA and other U.S. agencies' sites
JFF MORGES | JUNE 16, 2011
Hacking group LulzSec focuses embarrassing attacks on U.S. agencies; hacks CIA website, hits FBI Chicago and may have infiltrated the Senate again.

Security  **msnbc.com**
Hackers for hire: Criminals offer services online
DDoS attacks can be launched for average of \$5 to \$10 per hour, researcher finds.
JENNIFER N. LITTELL | 6:10:07 PM ET

TECHLAND
LulzSec Knocks 'Minecraft,' 'EVE Online,' 'League Of Legends' and 'The Escapist' Offline
By Matt Peckham on June 14, 2011

The Register
Anonymous unsheathes new, potent attack weapon
Better DDoS attacks ahead
By John Leyden • Get more from this author
Posted in Enterprise Security, 4th August 2011 11:17 GMT

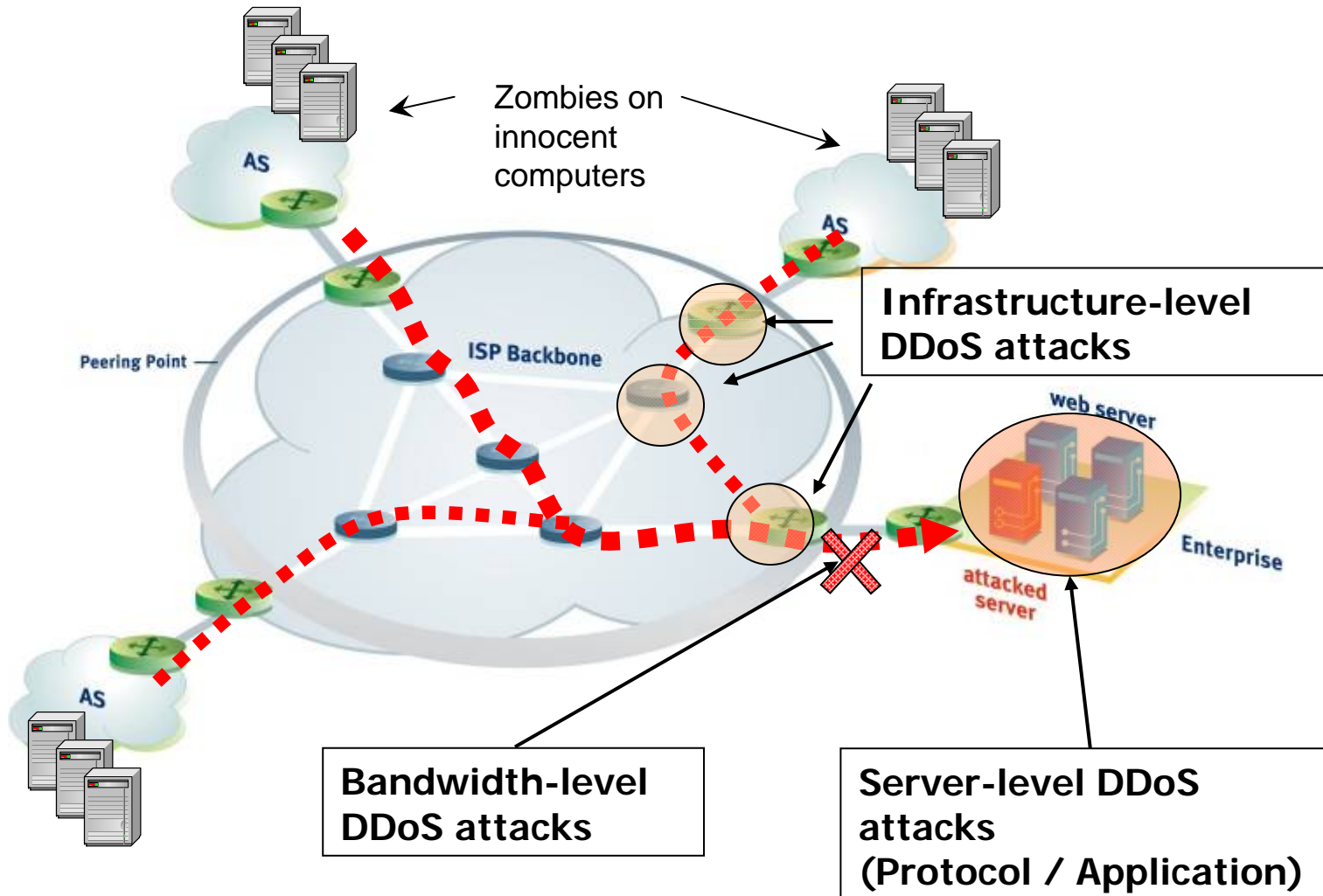
infosec ISLAND
Anonymous Launches DDoS Attack on USChamber.com
Tuesday, May 24, 2011

BBC Mobile 20 June 2011 Last updated at 15:32 ET
Soca website taken down after LulzSec 'DDoS attack'
The UK Serious Organised Crime agency has taken its website offline after it appeared to be a victim of an attack by hacking group Lulz Security.

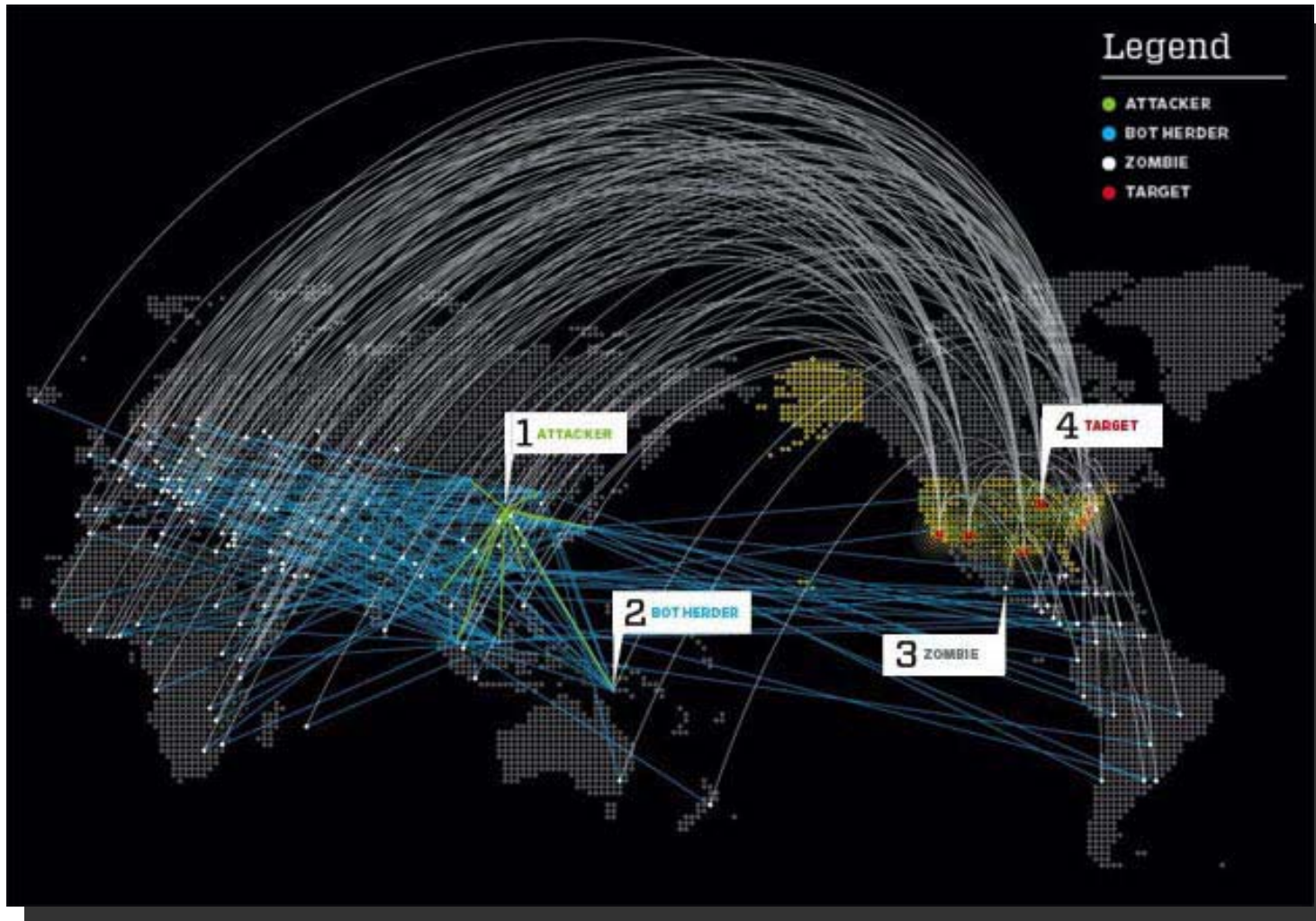
What is DDoS

- A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
- The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

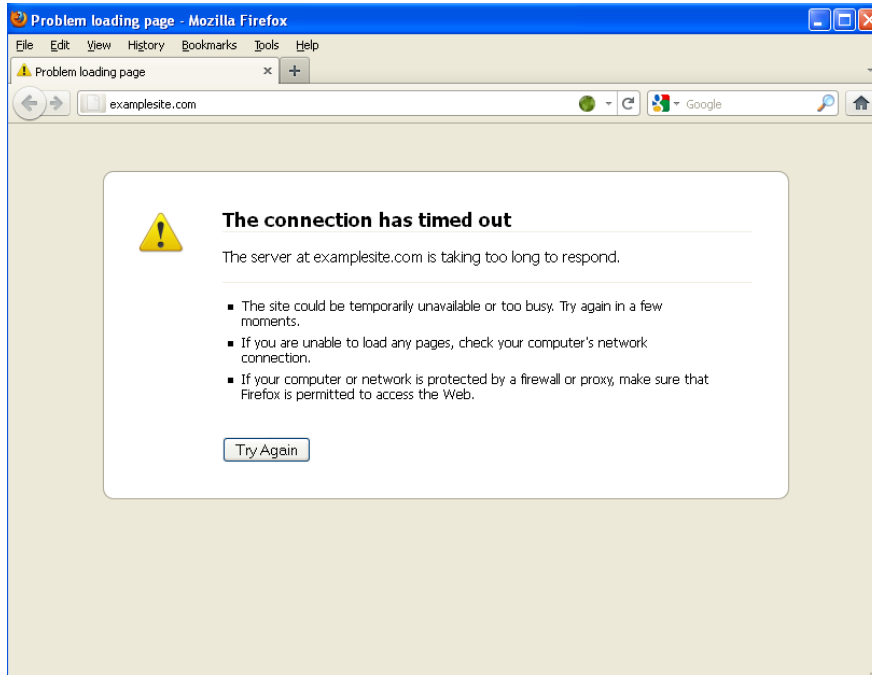
What is DDoS



What is DDoS



What does DDoS look like



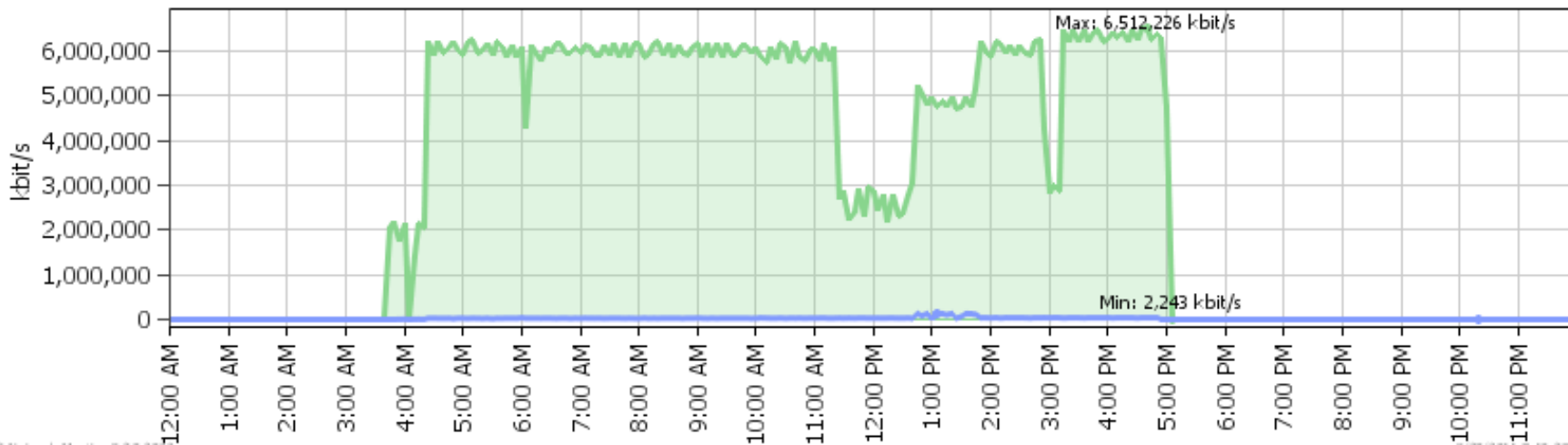
Client

- Website loading very slow
- Page can not be opened or shows an error page
- Transaction timeout / failure

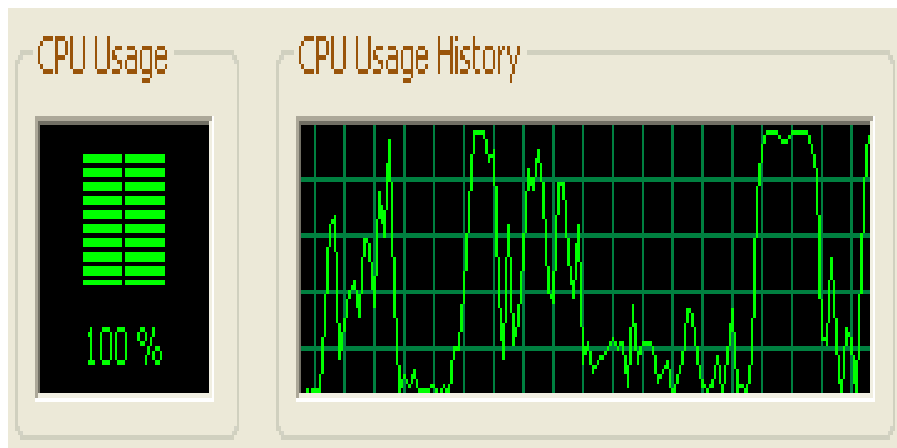
What does DDoS look like

ISP

- Sudden increase of traffic
- Customers complain inaccessibility to website
- Router CPU / Memory high
- Packet loss



What does DDoS look like

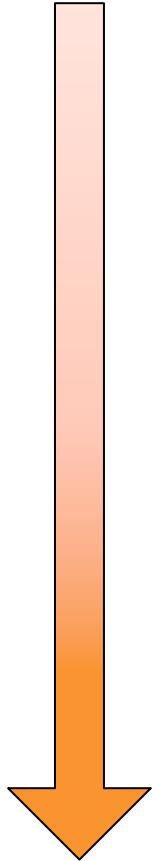


Corporate Network Operator

- Traffic spike
- Slow Server response
- Large amounts of log files
- CPU high
- Memory high
- Server reboot
- Other services impacted
- Clients complain

Impact of DDoS attack

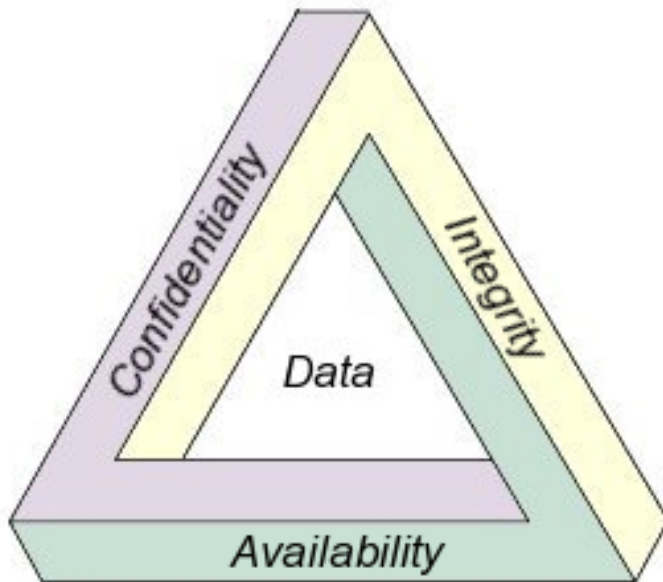
Normal Service



- Higher bandwidth usage (pay more to ISP)
- Website loading slow (carried by another ISP)
- Website loading very slow (ISP line congested, server busy)
- Website sometimes fail (server busy, DB busy)
- Web Server hang
- Router reboot
- Server reboot
- Other services down

Service Down

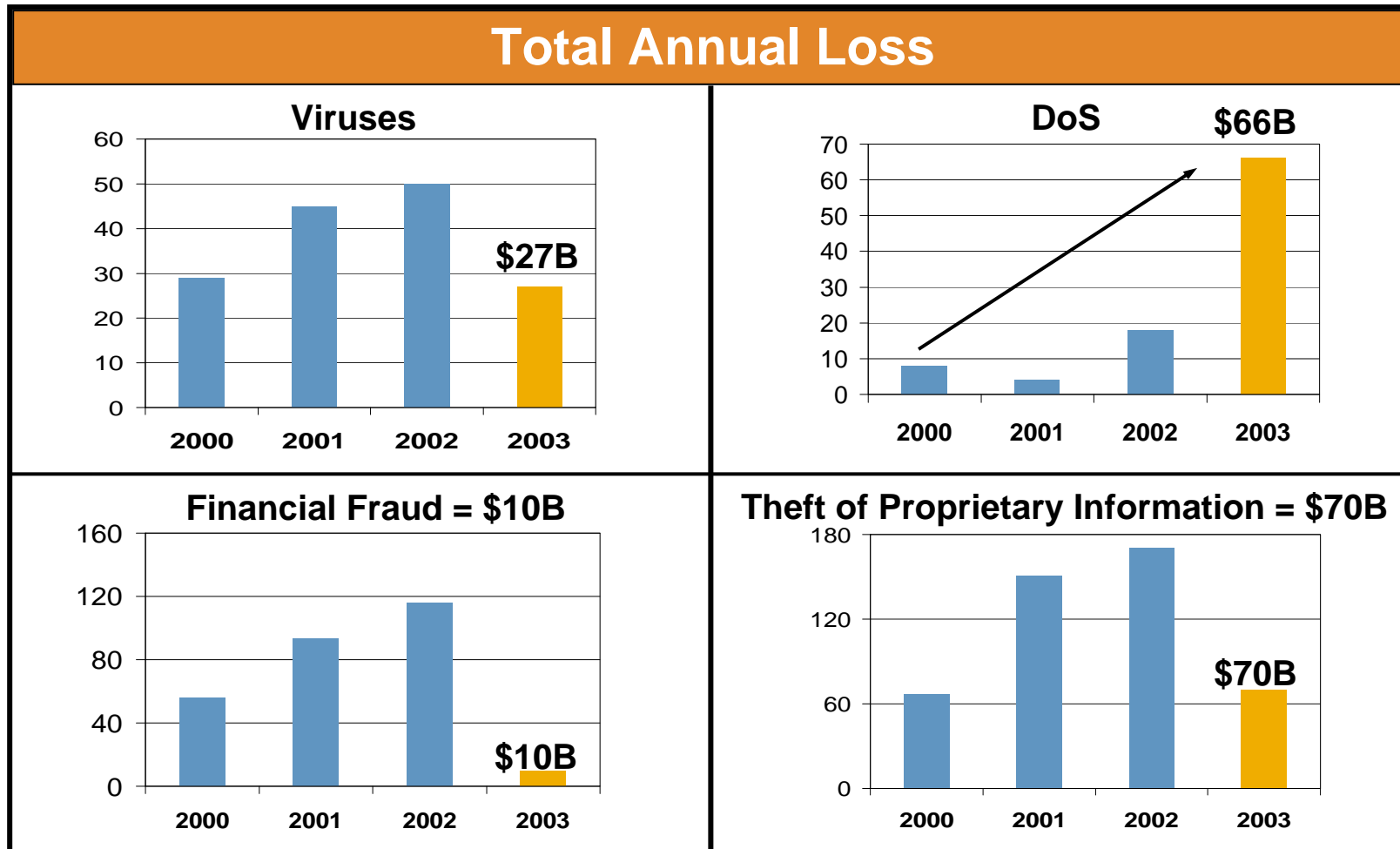
Impact of DDoS attack



Availability

- Without Availability, Confidentiality and Integrity are “Not Available”
- The goal of DDoS attack is to DENY your service to the public, including attackers
- DDoS is not only from internet, also can originate from internal sources

Impact of DDoS attack



Source: 2003 CSI/FBI Computer Crime & Security Survey

Impact of DDoS attack



- Governments and Organizations
 - Reputation
- Commercial
 - Reputation
 - Custom confidence
 - Loss of business

Who will be under risk of DDoS

- 1 Government website
- 2 Organizations
- 3 Financial Service Institutes
- 4 Online Gaming
- 5 Online transctions
- 6 Online Gambling
- 7 Information site
- 8 Search Engine
- 9 Social Network

Type of attacks

	Bandwidth Flood	Protocol / Application
Goal	<ul style="list-style-type: none">▪ Attack to congest your network	<ul style="list-style-type: none">▪ Attack on vulnerability of protocol or application
Common attack types	<ul style="list-style-type: none">▪ UDP Flood▪ ICMP flood▪ Malformed traffic	<ul style="list-style-type: none">▪ TCP SYN flood▪ HTTP GET flood▪ DNS Query flood
Post-attack impact	<ul style="list-style-type: none">▪ Services resume after attack	<ul style="list-style-type: none">▪ Services may not resume after attack

Who is attacking

It is just extension of real war



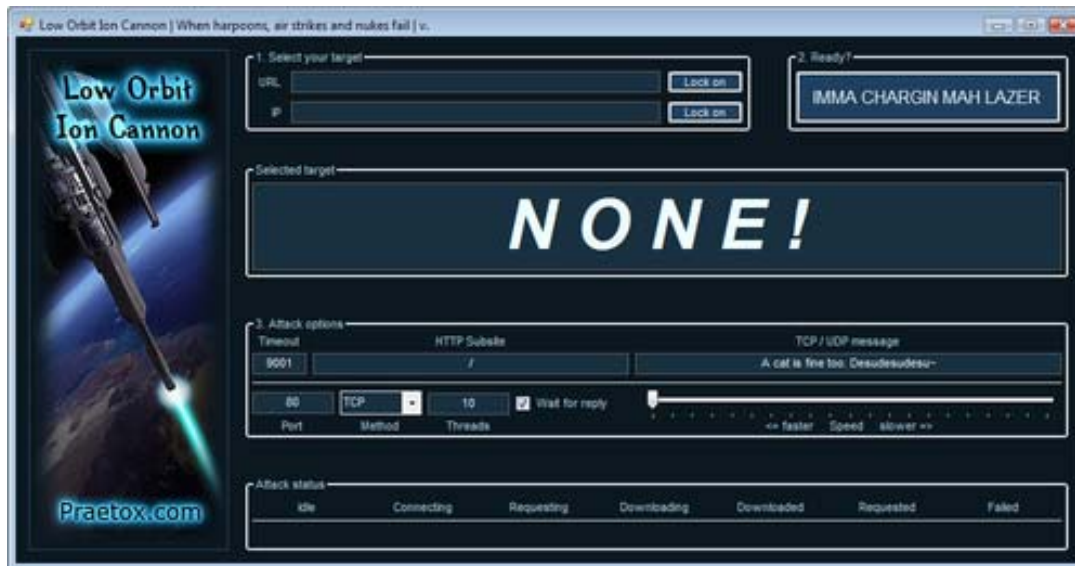
Possible Attackers

- Competitor
- Ex-employee
- Script Kiddies
- Commercial (hired) attacker
- Blackmailers

Why DDoS is so popular

Attack Tools

- Some can be obtained from internet for free
- Attack tools are becoming sophisticated



Why DDoS is so popular



More zombies available

- More users online everyday
- Millions of infected machines
- Users are not aware machine was participating in attack (as small as 1 packet per second)

Why DDoS is so popular

Higher Bandwidth

- Bandwidth is getting cheap
- Now home broadband can reach 1Gbps



Why DDoS is so popular



Commercial Attacker

- Cheap and readily available on the internet
- Offers “Attack by us” or “Attack by yourself”
- Some offers “post-paid” attack service with “SLA”

Why DDoS is so popular



Hard to trace

- Using fake IP (Spoof IP)
- Using zombies
- Using Proxy
- Using underground network
- Hire someone else
- Attack from internal source

DDoS Case Study

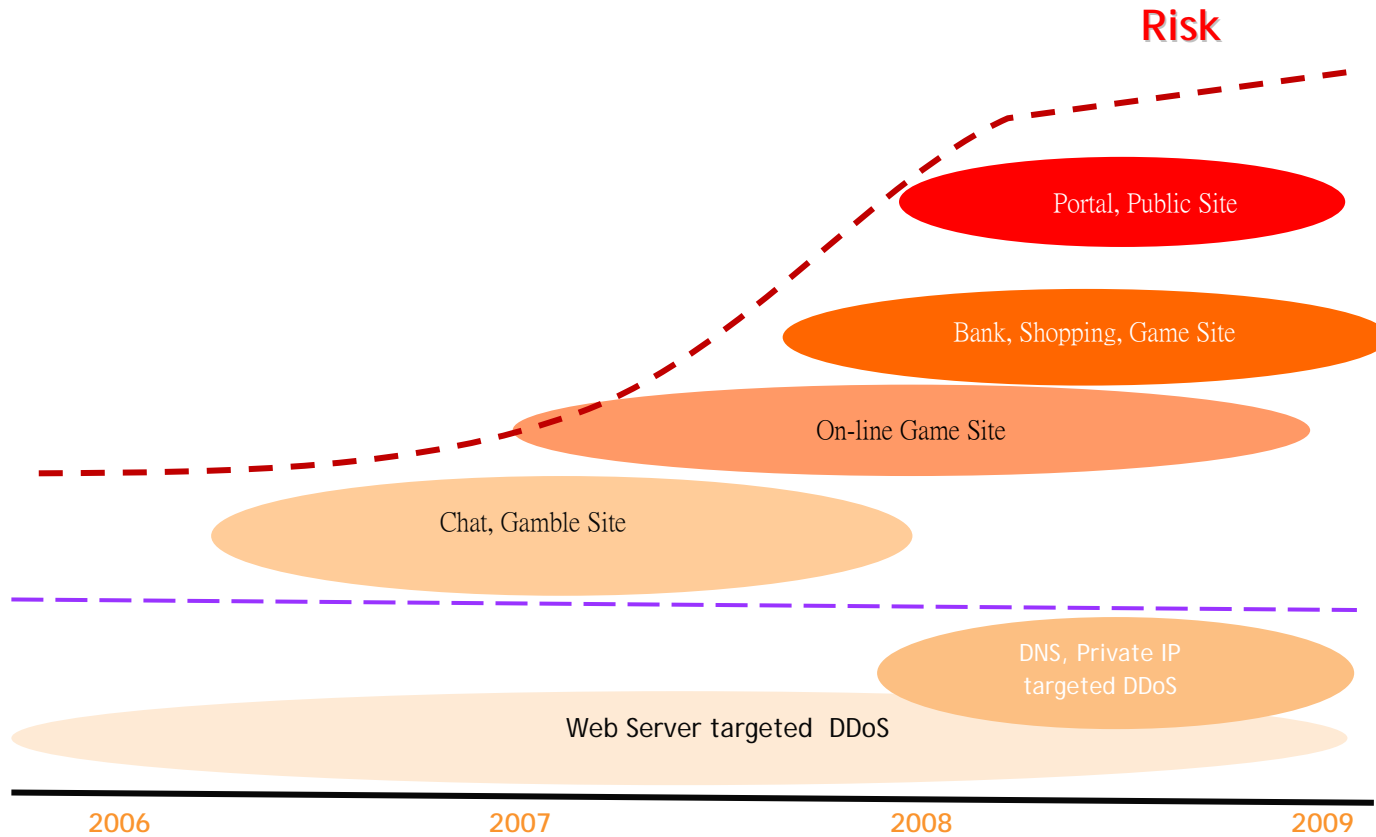
7.7 South Korean attack – History

- First DDoS attack is occurred in 2006
- Increase of target systems
 - - Small Websites → Major Websites(Bank, Portal, ...)
- Increase of ransom DDoS
- Increase of Application-layer DDos attack (Above 50%)
 - - HTTP Get flooding, Slowloris, SIP flooding
 - - Network Bandwidth Consumption → System Resource Consumption
- Hard to detect and block App.-layer DDos attack
 - - Because Each Zombie PC generates small traffic, Hard to detect by legacy security solution.

Source:KISA

DDoS Case Study

7.7 South Korean attack – History



DDoS Case Study

7.7 South Korean attack – during attack

1st Attack

Date : '09.7.5 02:00 ~ '09. 7.5 14:00, '09.7.5 22:00 ~ '09. 7.6 18:00

Target : **(US) White House** + 4 web sites

(US) White House, Department of Homeland Security+ 19 web sites

2nd Attack

Date : '09.7.7 18:00 ~ 7.8 18:00, '09.7.7 21:00 ~ 7.8 07:00

Target : (US) White House, **NASDAQ**, Washington Post + 11 web sites

(KR) Blue House, Ministry of National Defense,
National Assembly, NAVER(Portal) + 7 web sites

3rd Attack

Date : '09.7.8 18:00 ~ '09.7.9 18:00

Target : (KR) Blue House, **National Cyber Security Center,**

DAUM(Portal), PARAN(Portal), + 11 web sites

4th Attack

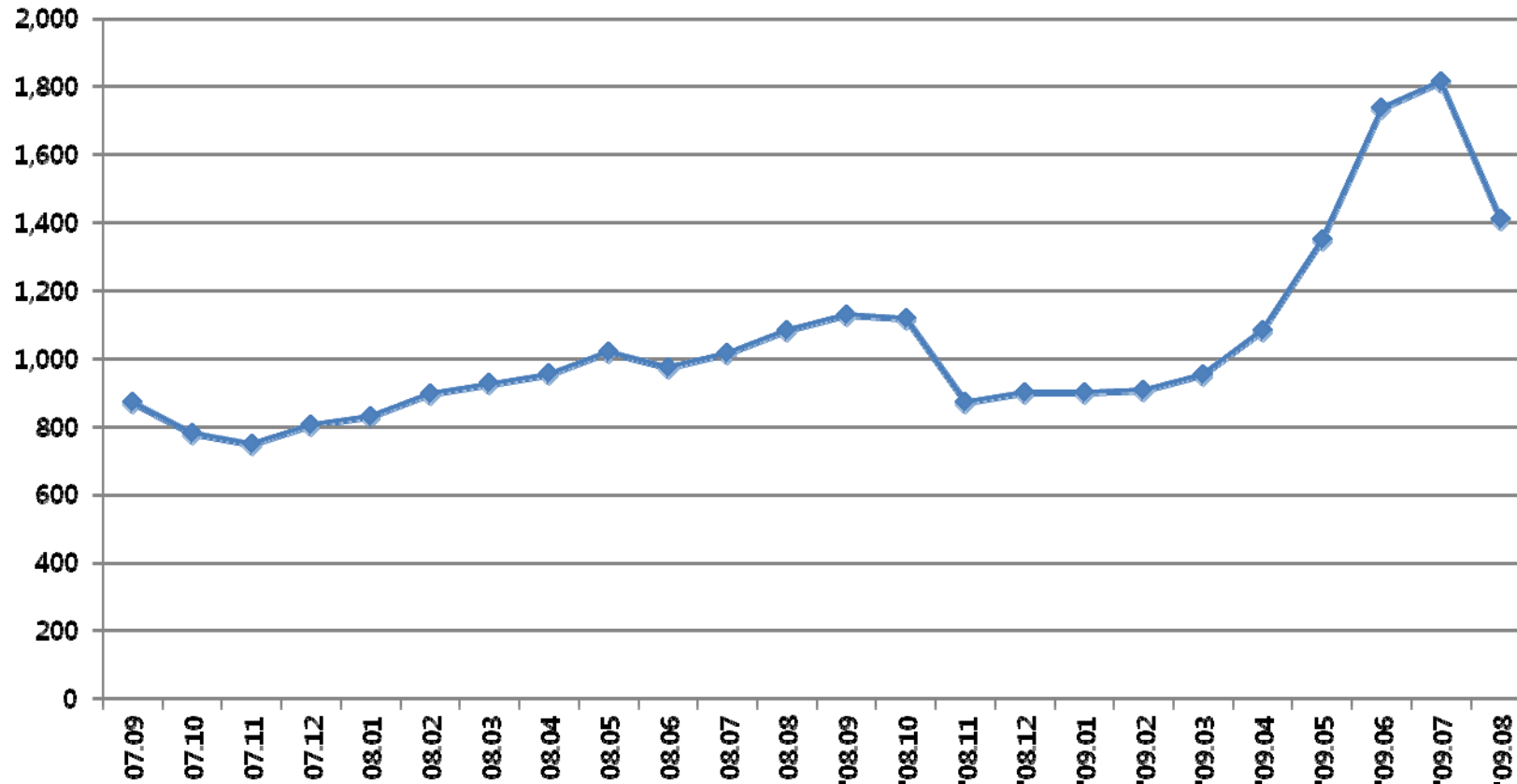
Date : '09.7.9 18:00 ~ '09.7.10 18:00

Target : (KR) NAVER(Portal), ChosunIlbo(Newspaper), G4C + 4 web sites

DDoS Case Study

7.7 South Korean attack – during attack

.kr DNS Query per day (Millions)



DDoS Case Study

7.7 South Korean attack - facts

Facts

- Start: 6PM July-06-2009
- End: July-09-2009
- Victims: 22 Korean sites, 14 US sites
- (Government, Bank)
- Lost: ~4-5b USD (33b KRW)
- Bot: 115,000
- C&C Server: 400
- Attack Type: DNS, ICMP, HTTP GET
- Attack Source: UNKNOWN

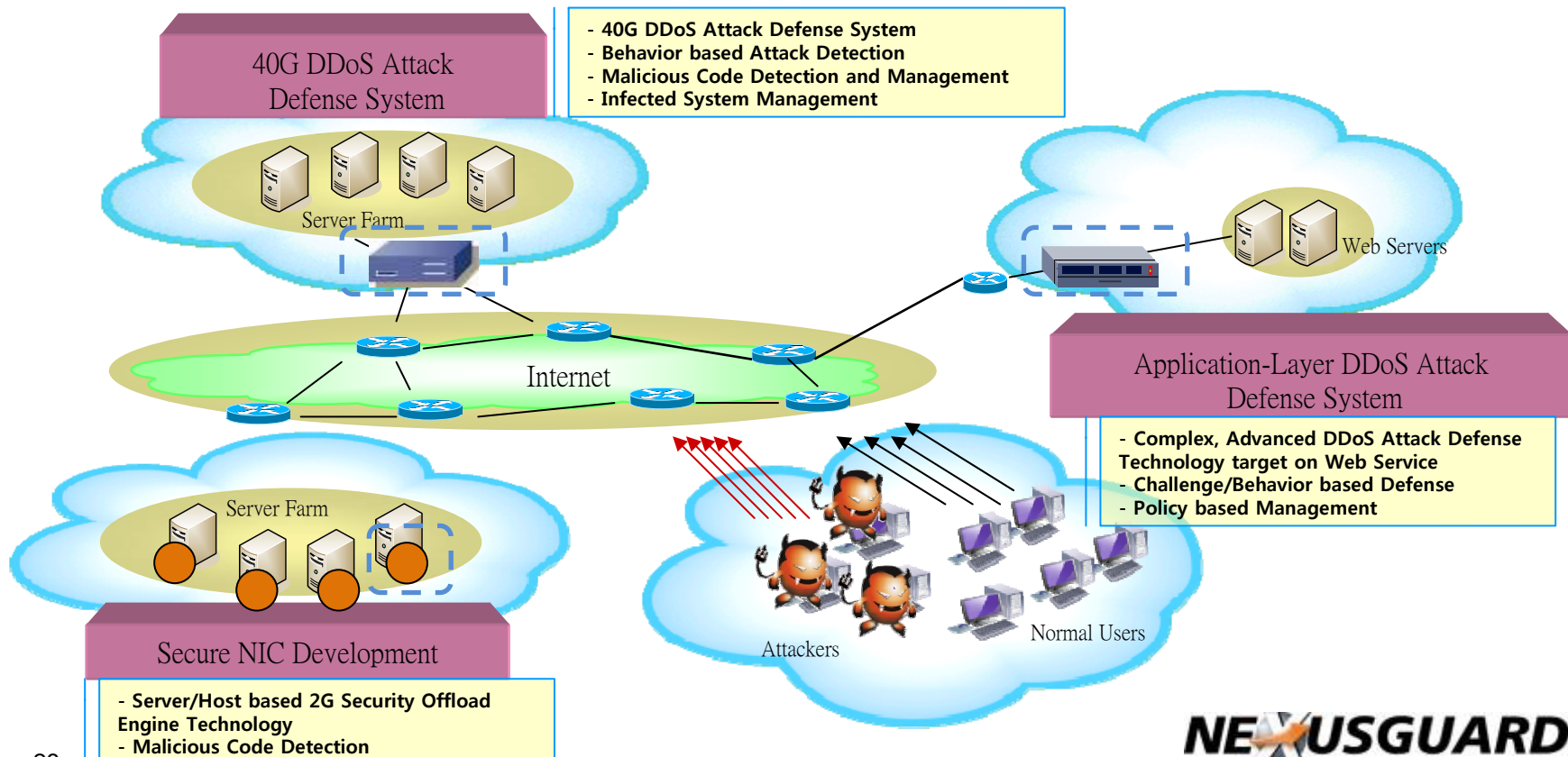
Aftermath

- Becomes breaking news/ headlines for a few weeks
- South Korean government deploys
 - 40G attack defense system
 - Application Layer attack defense system
 - Secure NIC

DDoS Case Study

7.7 South Korean attack – post attack countermeasure

- Objective
 - 40 Gbit DDoS Attack Defense System and Secure NIC Development
 - Advanced Application-Layer DDoS Attack Defense System targeted on Web Services



DDoS Case Study

7.7 South Korean attack – conclusion

- Information Sharing
 - Information Sharing is the most important factor for the success of effective incident prevention and response. For this purpose, we suggest improvements in the legal system and developing the technology found in Korea
- International Co-operation
 - Cyber attacks occur cross-border
 - Consensus is needed for monitoring, keeping logs, information sharing, and co-operation for cross-border incidents
- Awareness
 - It is difficult, but the most important for end-point security.
 - We should improve not only the legal framework but also awareness.

DDoS mitigation Solution

Blackhole

- Pros:
 - Effective instantly
 - Lowest in cost
 - Triggered by customer or ISP
- Cons:
 - No one else in the world can access
 - One IP each time
 - DDoS attack is successful

Router / Firewall

- Pros:
 - Deployed at customer edge
 - Full control of the device
- Cons:
 - Limited packet inspection
 - Expensive to deploy

DDoS mitigation Solution

Intrusion Prevention System (IPS)

- Pros:
 - Inspect all packets
 - Deep packet inspection
- Cons:
 - Process intensive
 - Expensive to invest and maintain

Content Delivery Network (CDN)

- Pros:
 - Distributed to multiple datacentres
 - One region down won't impact other regions
- Cons:
 - Does not filter or rate-limit traffic, just redirect to nearest region
 - Can be exploited to magnify the attack
 - Does not support once commercial quota is exhausted.

DDoS mitigation Solution

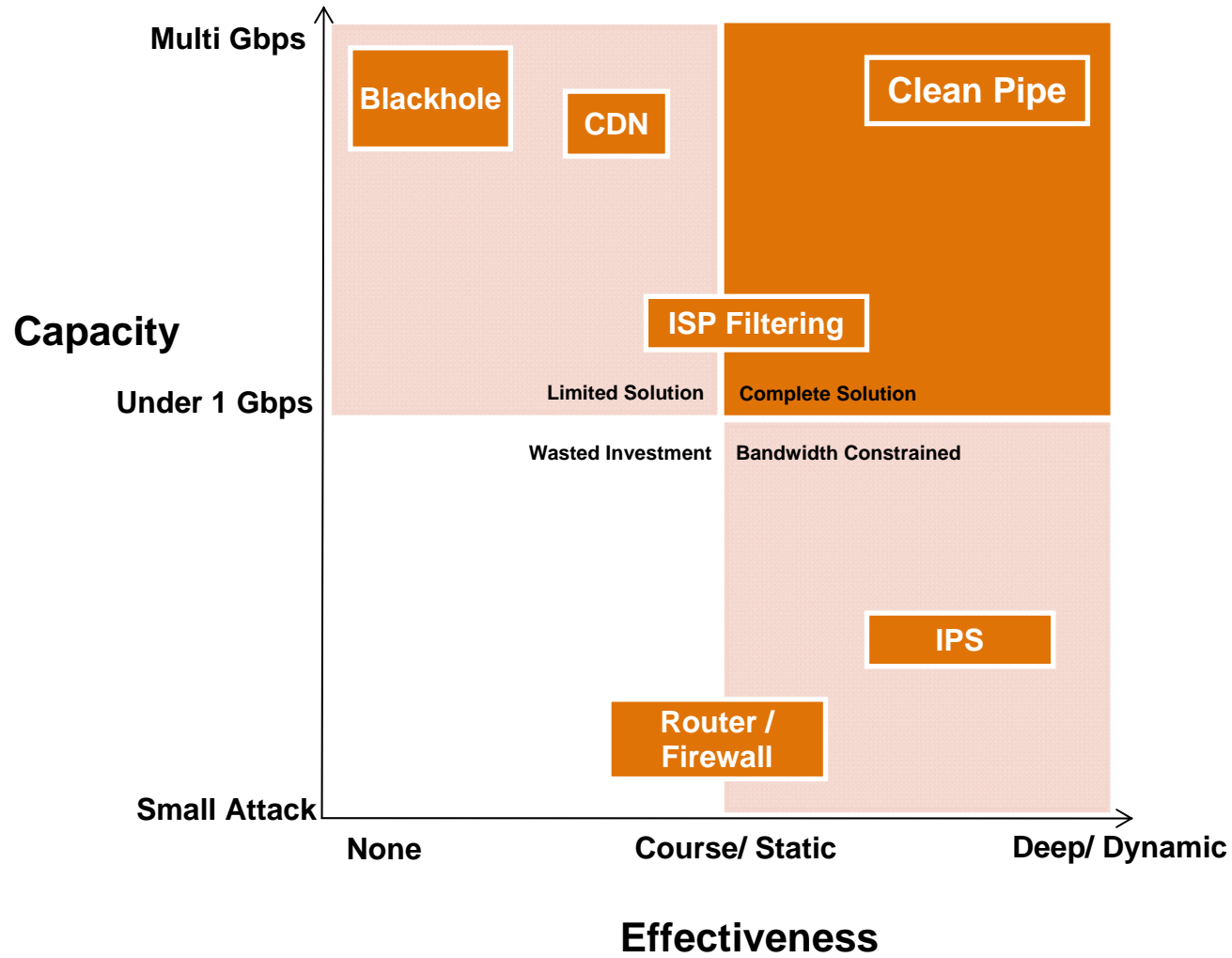
ISP Filtering

- Pros:
 - Easy to deploy at ISP side
- Cons:
 - Common filters only
 - Must be available and enabled on all ISPs
 - Must be “always on”
 - Network is designed to carry commercial traffic only

Clean Pipe

- Pros:
 - ISP agnostic
 - Can do packet filtering “on demand” or “always on”
 - Network is designed to carry and filter attacks
- Cons:
 - Usually more expensive

DDoS mitigation Solution



Tips – protect your PC / Server from becoming a zombie

- **Do not open suspicious emails**
- **Do not open suspicious URLs**
- **Do not download software from untrusted sites**
- **Software updates**
- **Turn off unwanted services**



Do You Have Any Questions?

Contact me at:
contact@nexusguard.com