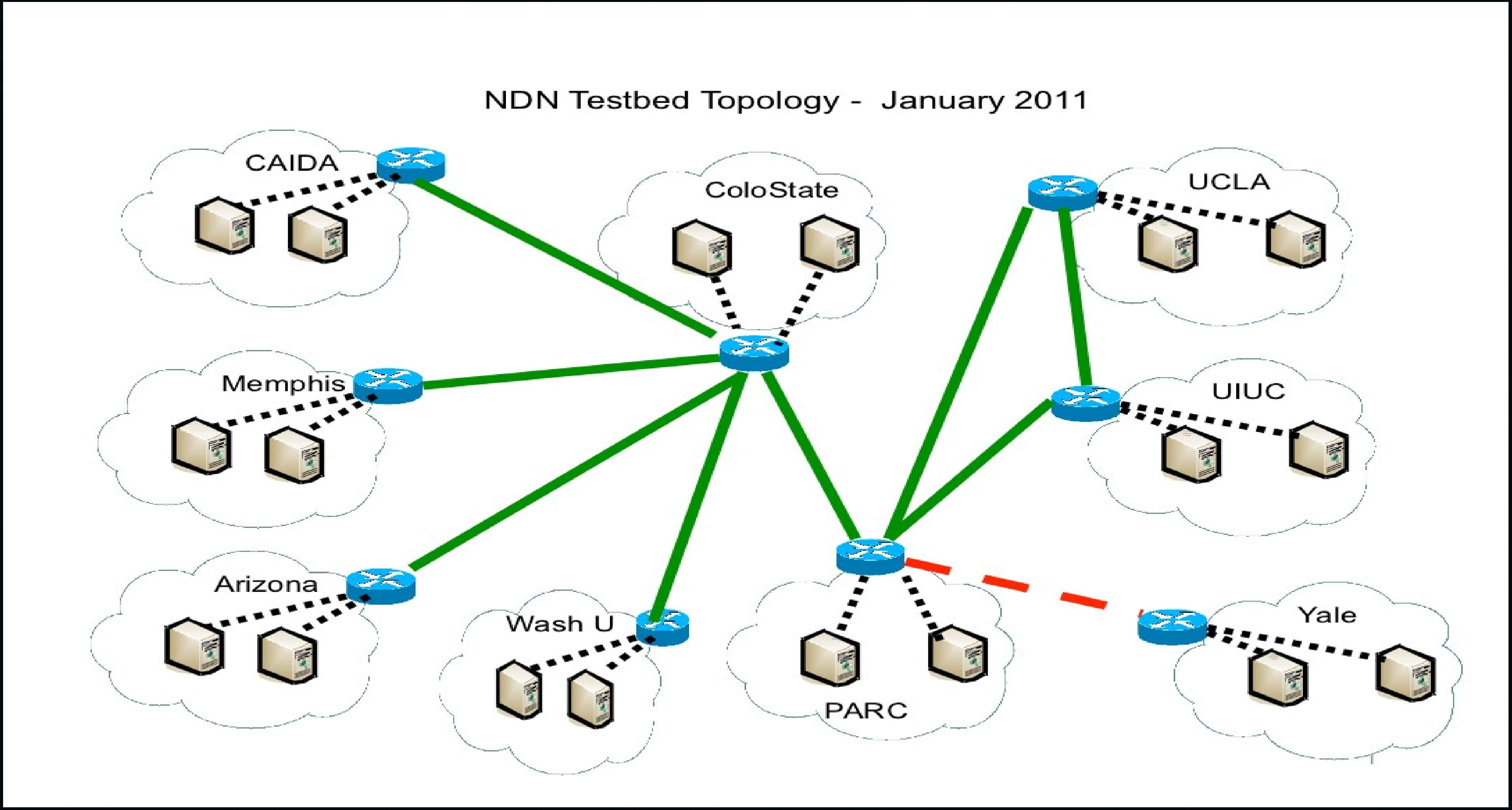
Distributed Denial of Service Attack (DDOS)

Presented By Bhupal Rai and Mrigendra K. Chaudhary

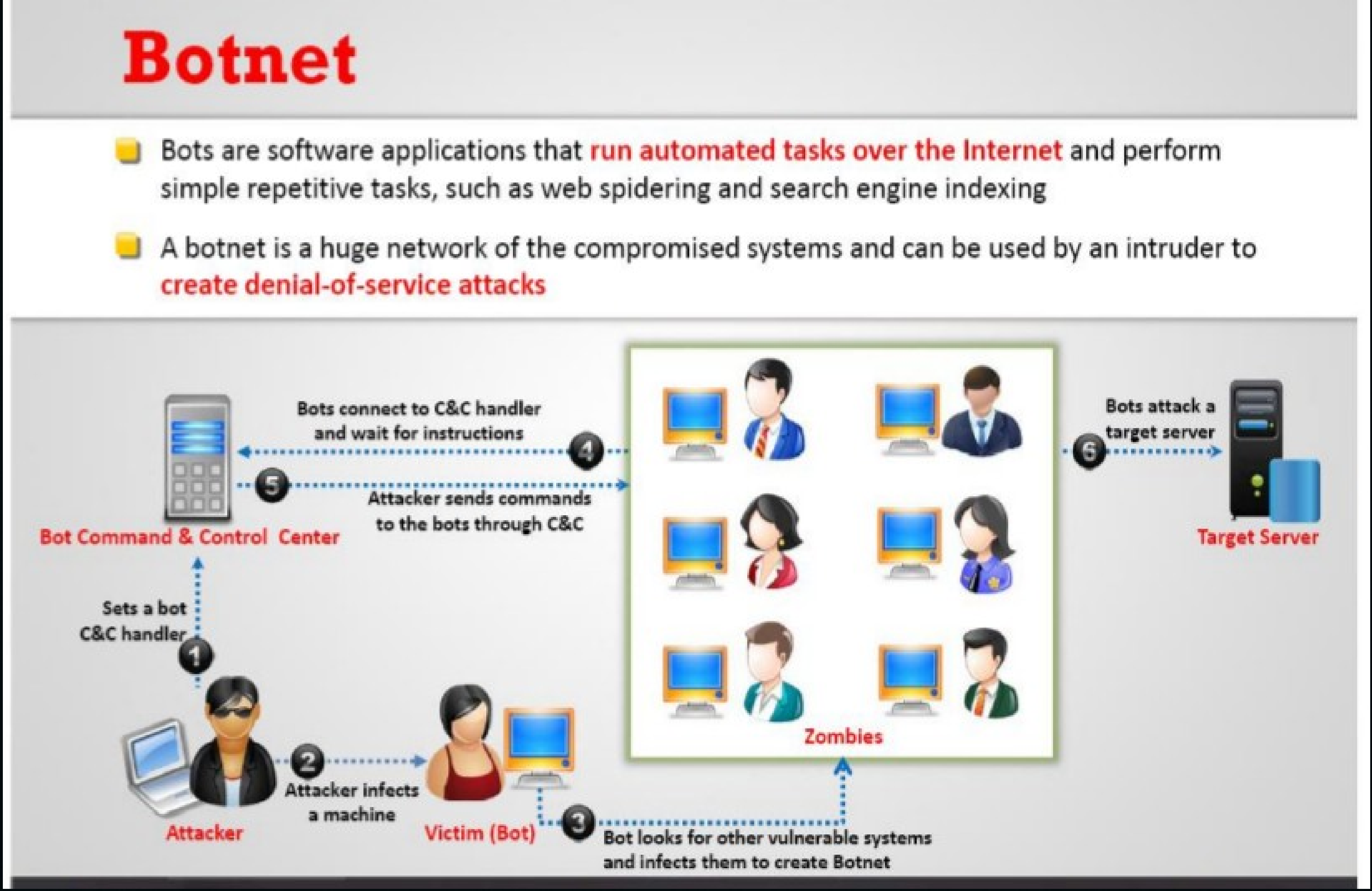
Network of networks Internet



Presented By Bhupal Rai and Mrigendra K.
Chaudhary

Some terms

- Bot
- Botnet
- Handler
- Zombi computer
- Flooding
- Service requests
- Server resource
- Network resources
- Port
- Connection establishment



Botnet

- Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks, such as web spidering and search engine indexing
- A botnet is a huge network of the compromised systems and can be used by an intruder to create denial-of-service attacks

Bot Command & Control Center

Bots connect to C&C handler and wait for instructions 4

5 Attacker sends commands to the bots through C&C

Zombies

6 Bots attack a target server

Target Server

Sets a bot C&C handler 1

Attacker

2 Attacker infects a machine

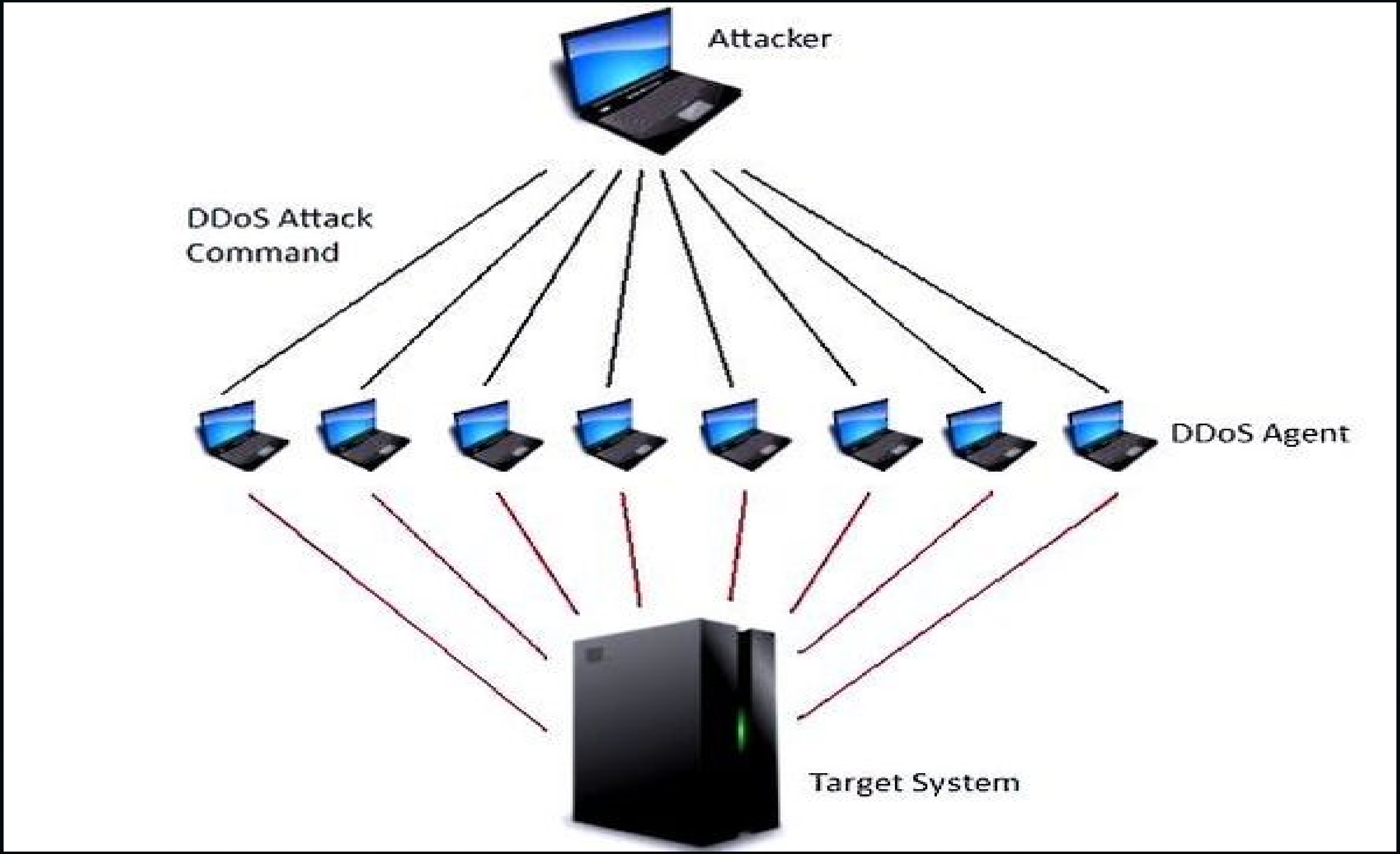
Victim (Bot)

3 Bot looks for other vulnerable systems and infects them to create Botnet

DDOS

- DOS attack
  - Denial of Service attack
  - An attempt to make a machine or network resource unavailable to its intended users
  - Done by single attacker using single connection or network

- DDOS attack
  - Distributed Denial of Service attack
  - The most sophisticated and easy to lunch cyber attack where an attacker tries to make server unavailable for legimate users
  - Network of remotely controlled compromised computer (botnet) are used to lunch attack.
  - Targets are mostly sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers


Attacker
DDoS Attack Command
DDoS Agent
Target System

DDOS Category

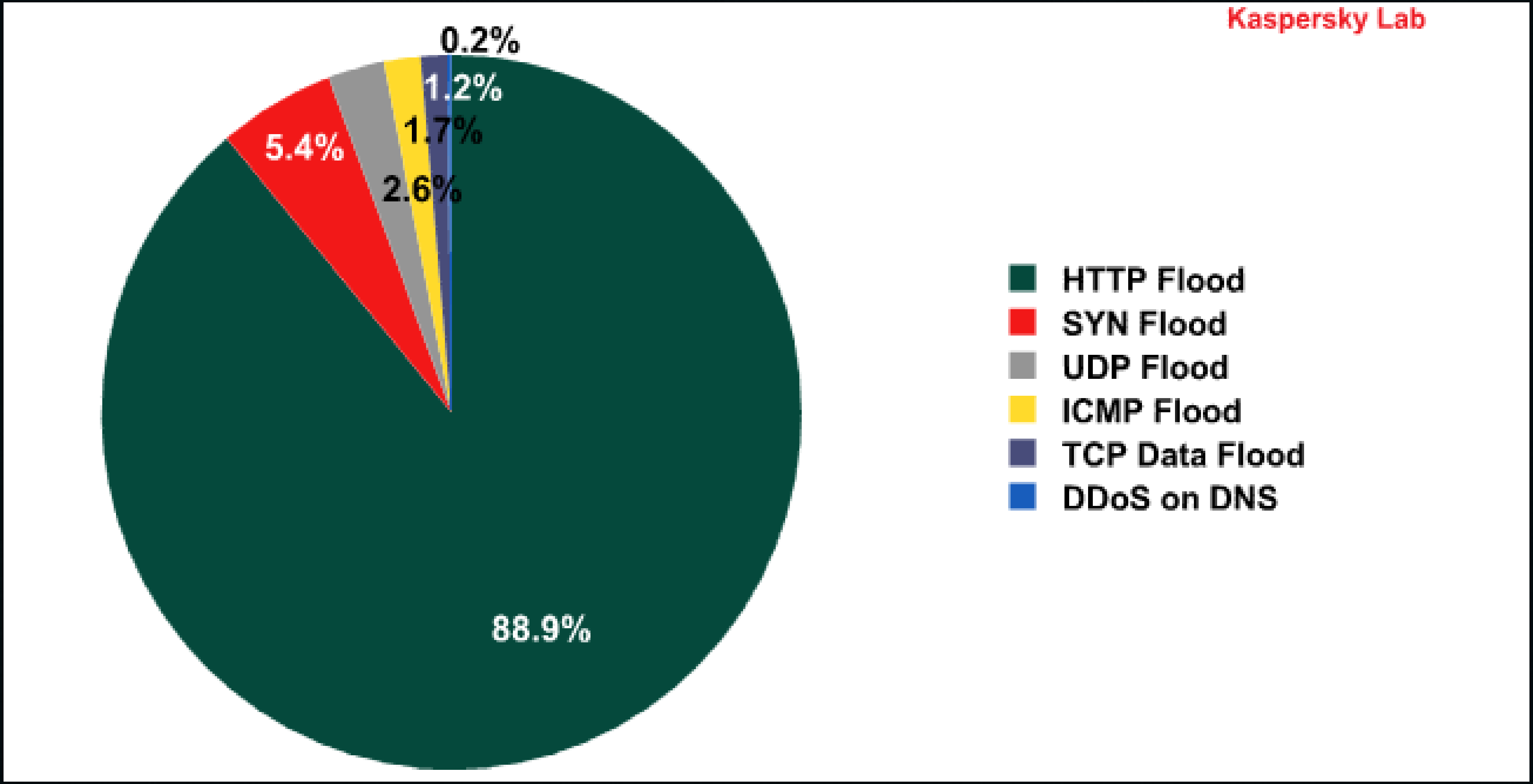
- Volume Based Attacks
  - Saturate target machine bandwidth
  - Aka. Layer ¾ Dos attack
  - UDP floods, ICMP floods, etc.

- Protocol Attacks
  - Consumes actual sever resources
  - SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more

DDOS Category

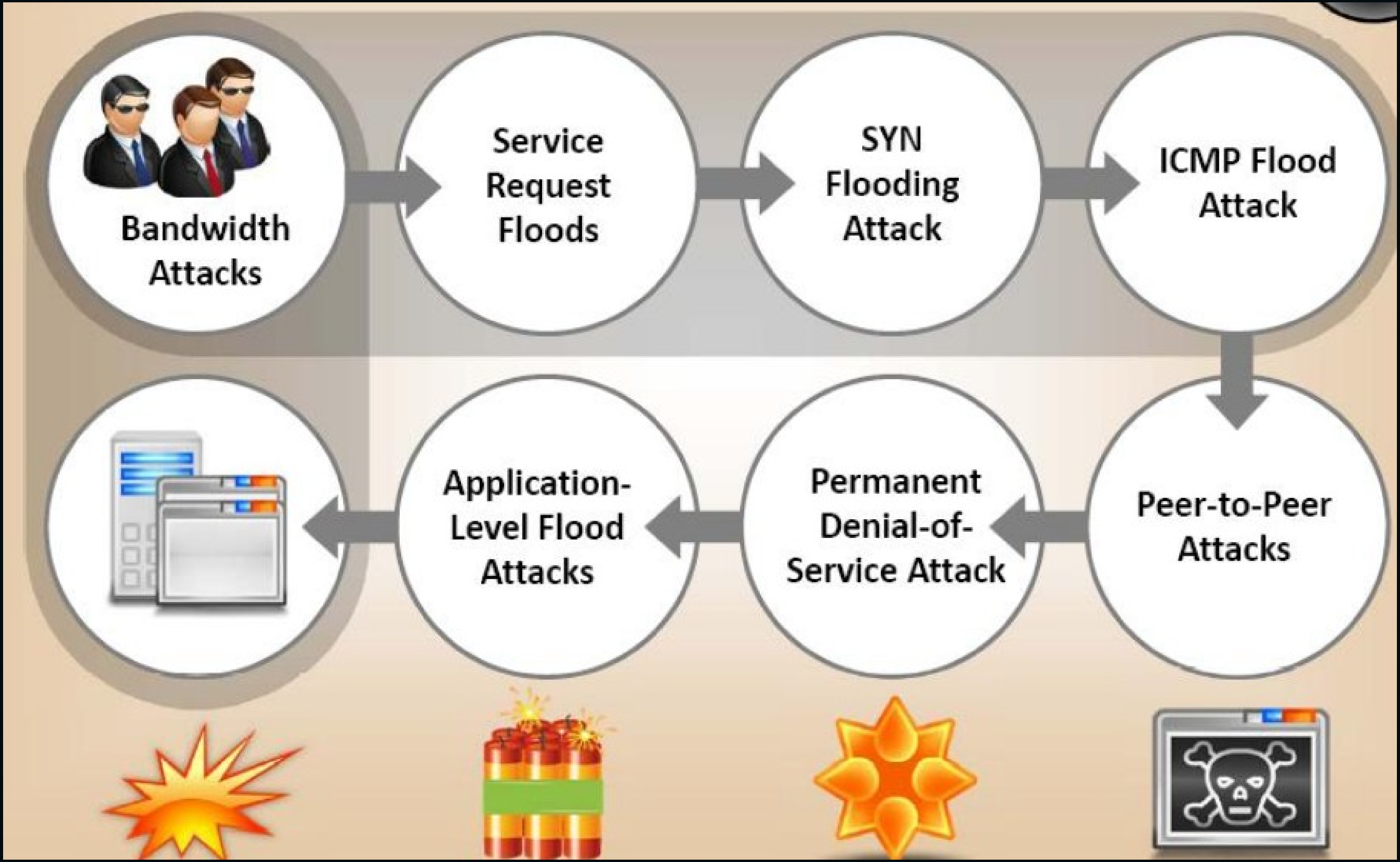
- Application Layer Attacks
  - More complicated attack
  - Aka. layer 7 DDoS attack
  - attackers target the application layer of the OSI model
  - may exploit vulnerabilities in application software

DDOS Types -Kaspersky Lab 2011



Presented By Bhupal Rai and Mrigendra K. Chaudhary

DDOS attack techniques



Bandwidth Attacks

Service Request Floods

SYN Flooding Attack

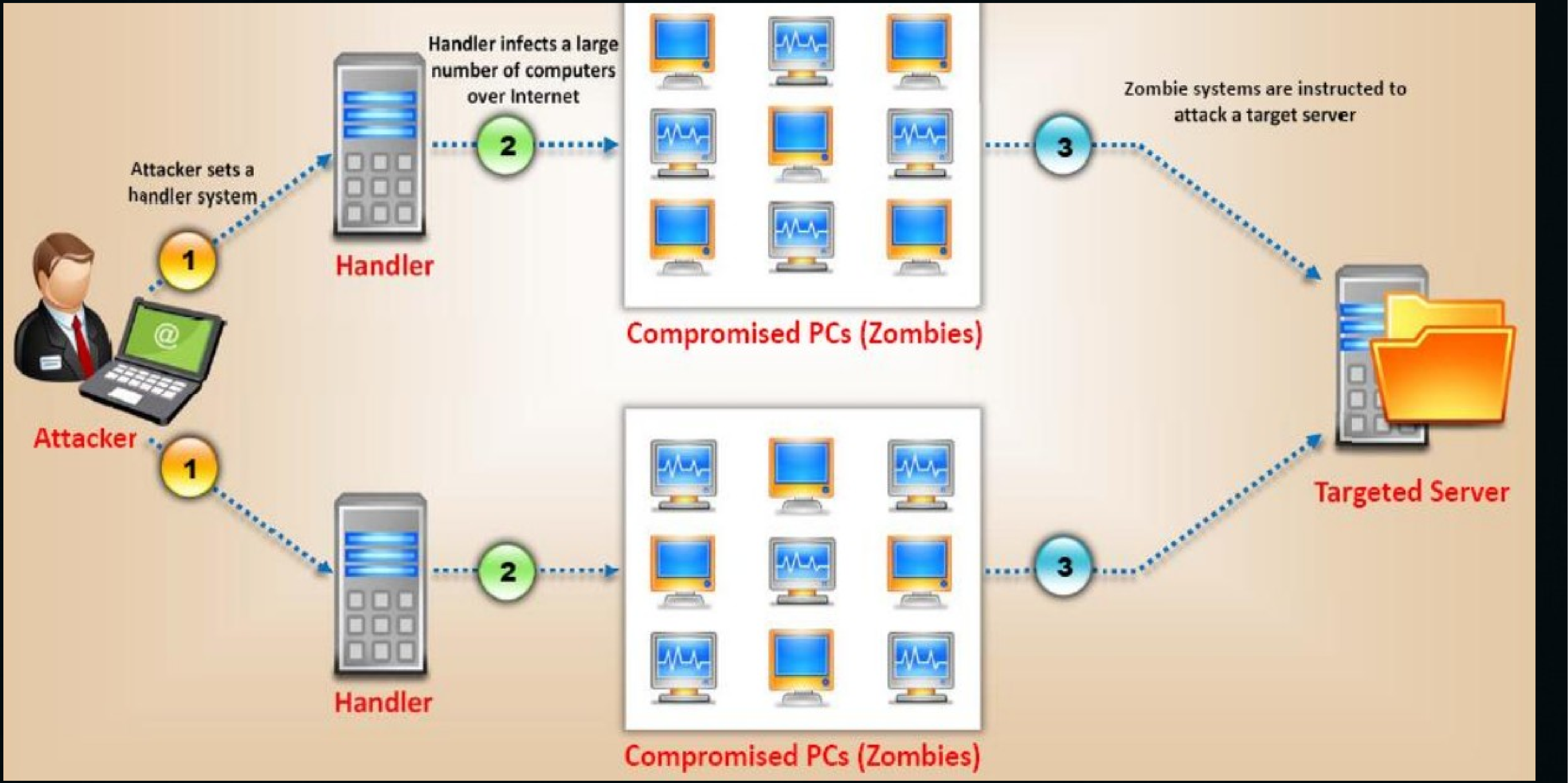
ICMP Flood Attack

Peer-to-Peer Attacks

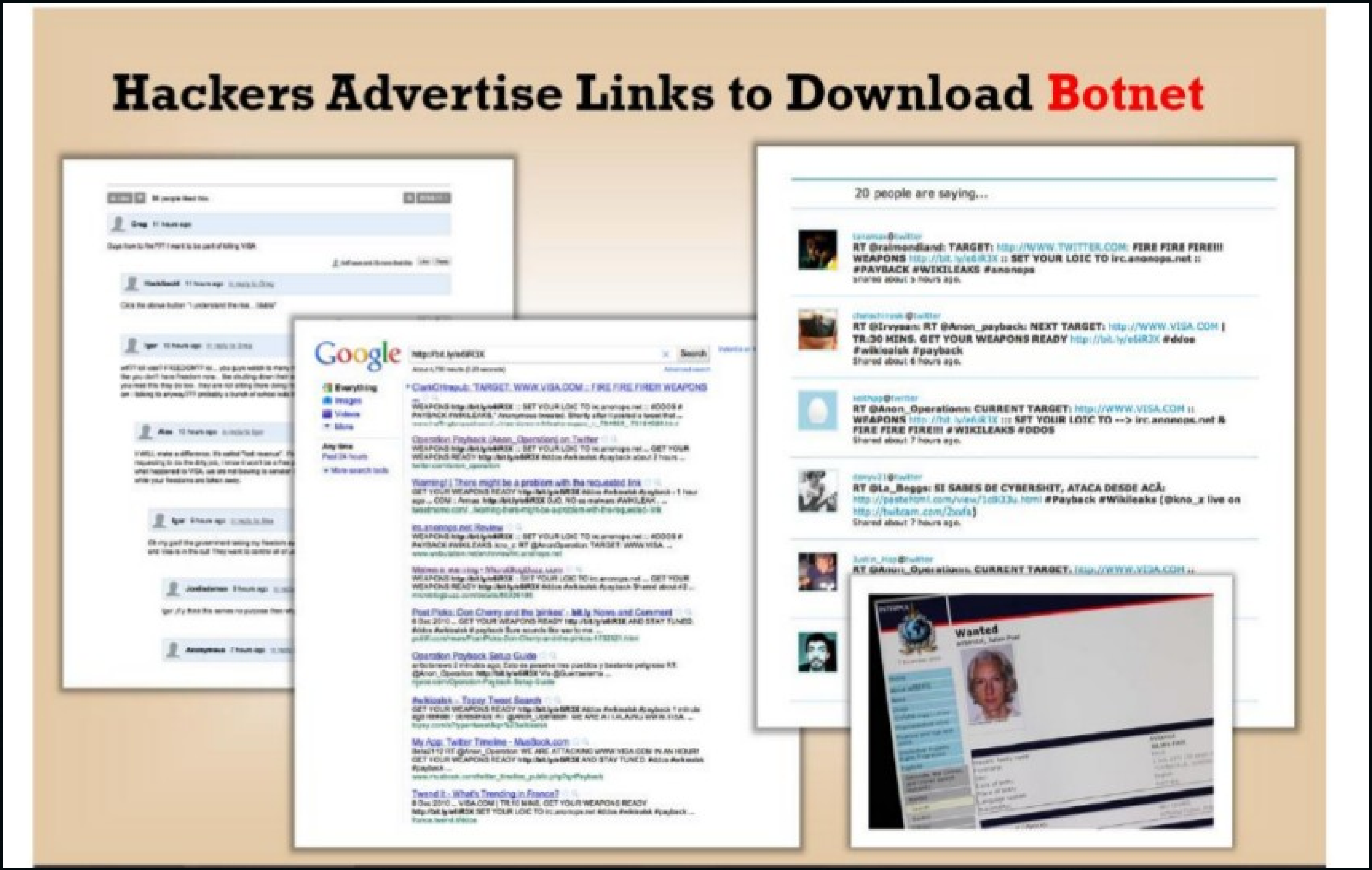
Permanent Denial-of-Service Attack

Application-Level Flood Attacks

How DDOS works


Handler infects a large number of computers over Internet
Attacker sets a handler system
1
2
3
Zombie systems are instructed to attack a target server
Handler
Compromised PCs (Zombies)
Attacker
1
2
3
Handler
Compromised PCs (Zombies)
Targeted Server

Presented By Bhupal Rai and Mrigendra K. Chaudhary



Hackers Advertise Links to Download Botnet

http://bit.ly/e6iR3X

20 people are saying...

RT @raimondland: TARGET: http://WWW.TWITTER.COM: FIRE FIRE FIRE!!! WEAPONS http://bit.ly/e6iR3X :: SET YOUR LOIC TO irc.anonops.net :: #PAYBACK #WIKILEAKS #anonops
Shared about 5 hours ago.

RT @Irvysan: RT @Anon_payback: NEXT TARGET: http://WWW.VISA.COM | TR:30 MINS. GET YOUR WEAPONS READY http://bit.ly/e6iR3X #ddos #wikileaks #payback
Shared about 6 hours ago.

RT @Anon_Operations: CURRENT TARGET: http://WWW.VISA.COM :: WEAPONS http://bit.ly/e6iR3X ::: SET YOUR LOIC TO --> irc.anonops.net & FIRE FIRE FIRE!!! #WIKILEAKS #DDOS
Shared about 7 hours ago.

RT @La_Beggs: SI SABES DE CYBERSHIT, ATACA DESDE ACÁ: http://pastehtml.com/view/1cdi33u.html #Payback #Wikileaks (@kno_z live on http://twitcam.com/2xafs)
Shared about 7 hours ago.

RT @Anon_Operations: CURRENT TARGET: http://WWW.VISA.COM ::

Demo