

# Denial-of-Service

Module 09

Unmask the Invisible Hacker.



# Module Objectives

CEH  
Certified Ethical Hacker

- Overview of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- Understanding Different DoS/DDoS Attack Techniques
- Understanding the Botnet Network



- Understanding Various DoS and DDoS Attack Tools
- Understanding Different Techniques to Detect DoS and DDoS Attacks
- DoS/DDoS Countermeasures
- Overview of DoS Attack Penetration Testing



# Module Flow



1

**DoS/DDoS Concepts**

2

**DoS/DDoS Attack Techniques**

3

**Botnets**

4

**DDoS Case Study**

5

**DoS/DDoS Attack Tools**

6

**Countermeasures**

7

**DoS/DDoS Protection Tools**

8

**DoS/DDoS Penetration Testing**

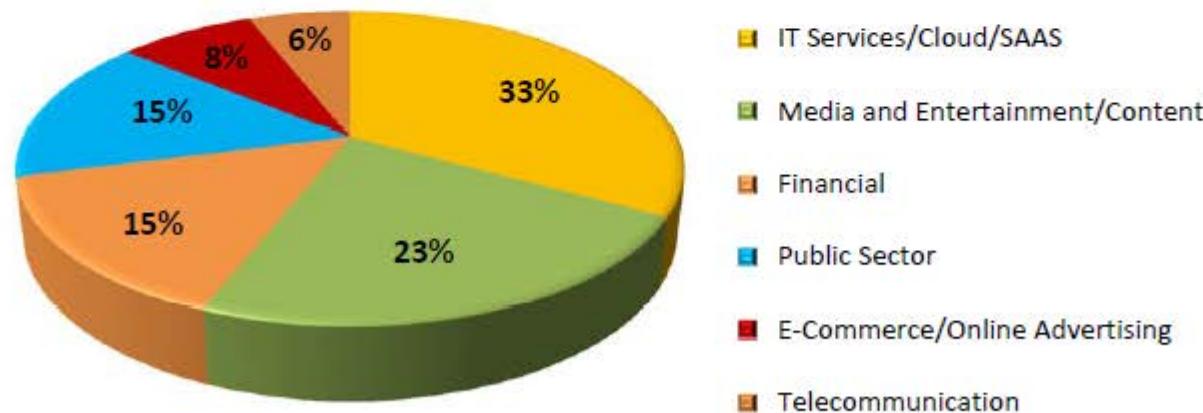
# DDoS Attack Trends

C|EH  
Certified Ethical Hacker

According to Verisign DDoS Trends Report – Q4 2014

Average attack size increased to **7.39** gigabits per second (Gbps), rising **14%** higher than in Q3 2014 and **245%** higher than Q4 2013

Mitigations By Industry Vertical - Q4 2014

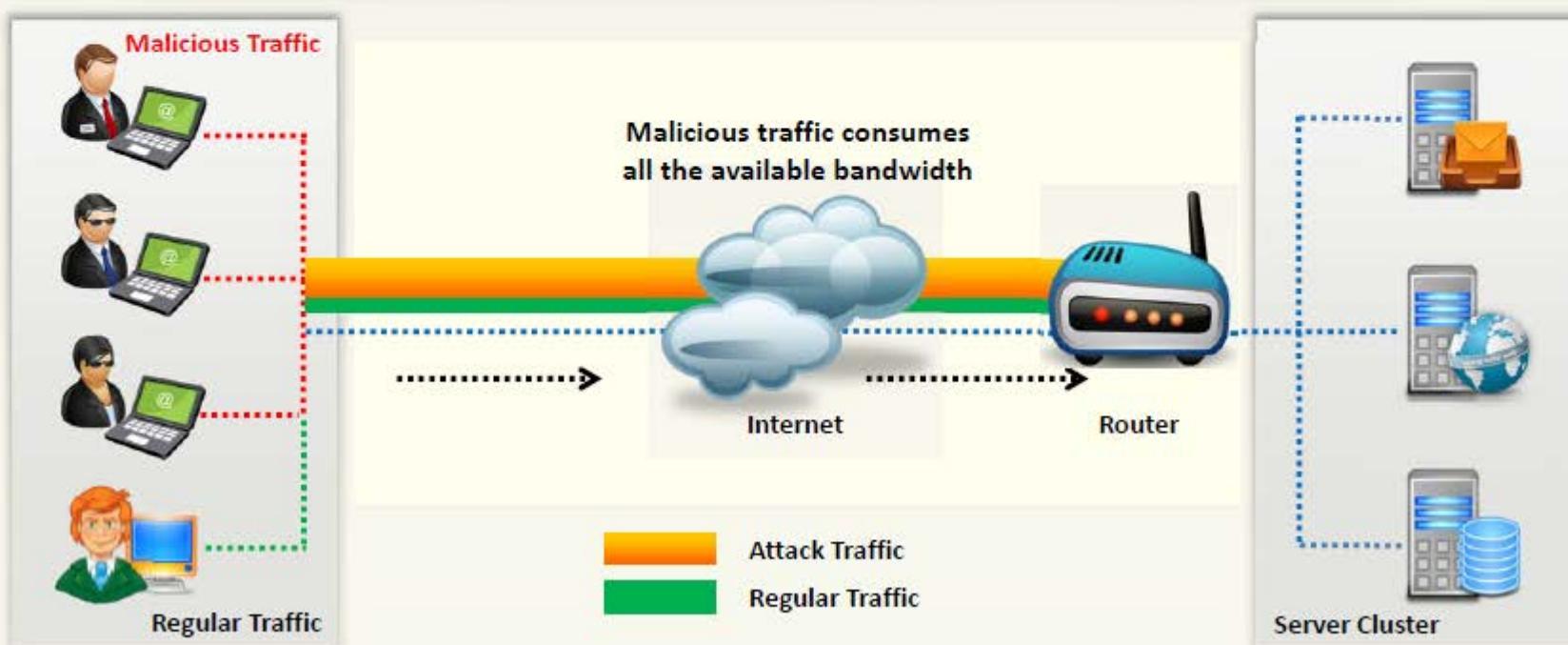


<https://www.verisigninc.com>

# What is a Denial-of-Service Attack?

CEH  
Certified Ethical Hacker

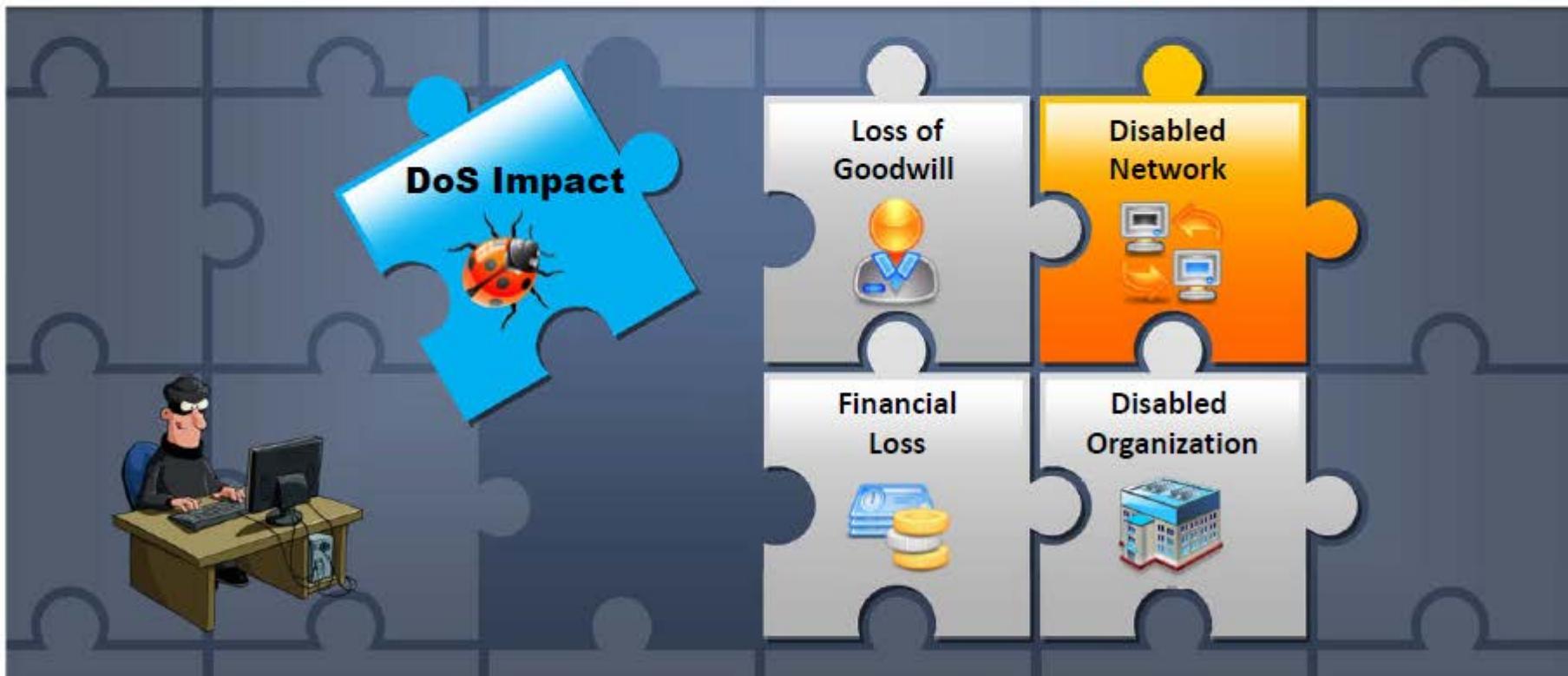
- Denial of Service (DoS) is an attack on a computer or network that **reduces, restricts** or **prevents** accessibility of system resources to its legitimate users
- In a DoS attack, attackers flood a victim system with **non-legitimate service requests or traffic** to overload its resources
- DoS attack leads to **unavailability of a particular website** and **slow network performance**



# What are Distributed Denial of Service Attacks?

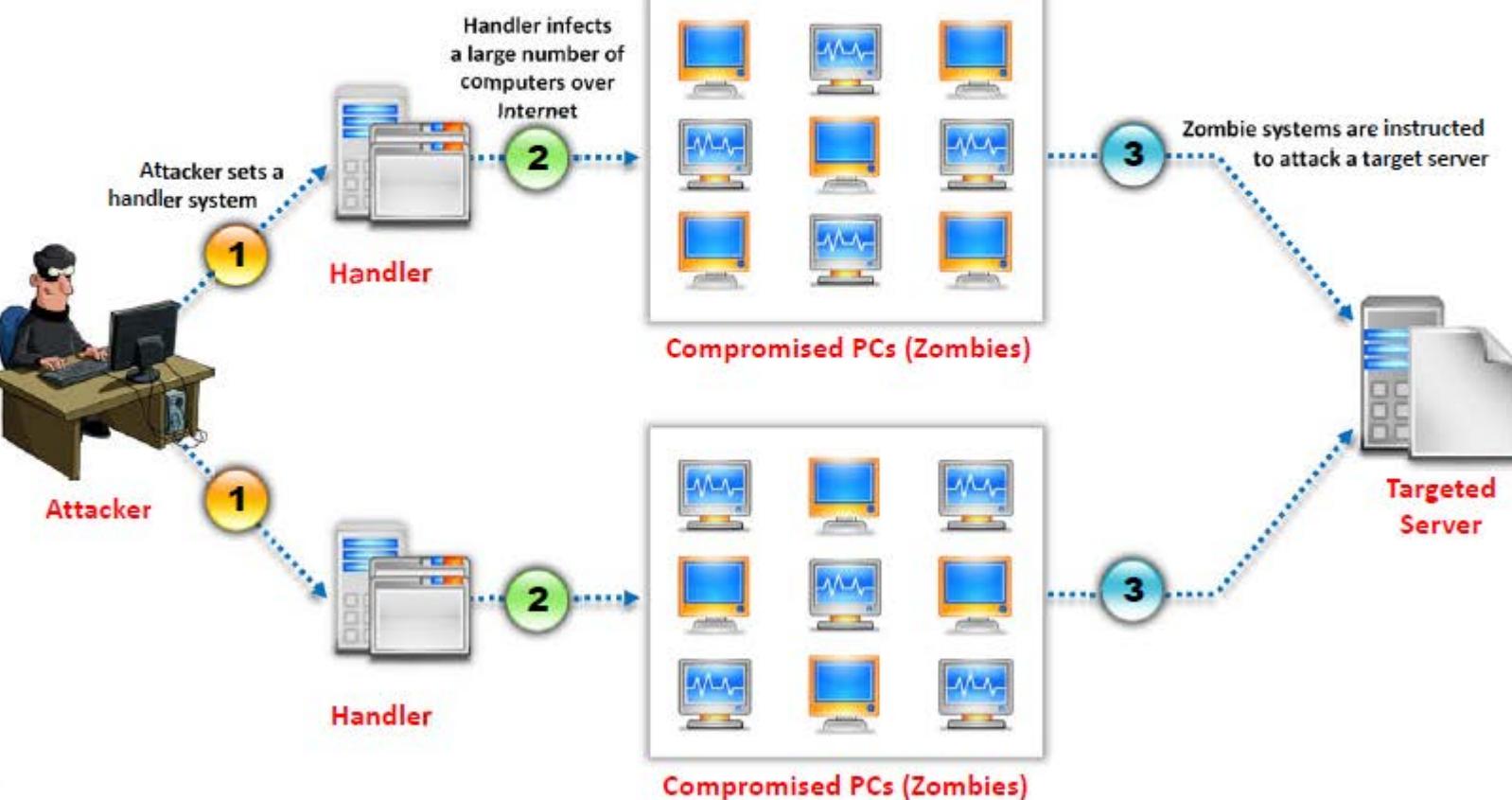
CEH  
Certified Ethical Hacker

- A distributed denial-of-service (DDoS) attack involves a **multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**



# How Distributed Denial of Service Attacks Work

**C|EH**  
Certified Ethical Hacker



# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

**6 Countermeasures**

**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# Basic Categories of DoS/DDoS Attack Vectors

**C|EH**  
Certified Ethical Hacker

## Volumetric Attacks

Consumes the **bandwidth** of target network or service



## Fragmentation Attacks

Overwhelms target's ability of re-assembling the **fragmented packets**



## TCP State-Exhaustion Attacks

Consumes the **connection state tables** present in the network infrastructure components such as **load-balancers**, **firewalls**, and **application servers**

## Application Layer Attacks

Consumes the **application resources** or service thereby making it unavailable to other legitimate users



# Bandwidth Attacks

01

A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses **several computers to flood a victim**



02

When a DDoS attack is launched, flooding a network, it can cause network equipment such as **switches** and **routers** to be overwhelmed due to the significant statistical change in the **network traffic**



03

Attackers use botnets and carry out DDoS attacks by flooding the network with **ICMP ECHO packets**



04

Basically, all bandwidth is used and no bandwidth remains for **legitimate use**



# Service Request Floods



An attacker or group of zombies attempts to **exhaust server resources** by setting up and tearing down TCP connections



Service request flood attacks flood servers with a **high rate of connections** from a valid source



It initiates a **request on every connection**

# SYN Attack

01

The attacker **sends a large number of SYN request** to target server (victim) with fake source IP addresses



02

The target machine **sends back a SYN ACK** in response to the request and waits for the ACK to complete the session setup



03

The target machine does not get the response because the **source address is fake**



**Note:** This attack exploits the **three-way handshake** method

# SYN Flooding

1

SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**

2

When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "**listen queue**" for at least 75 seconds

3

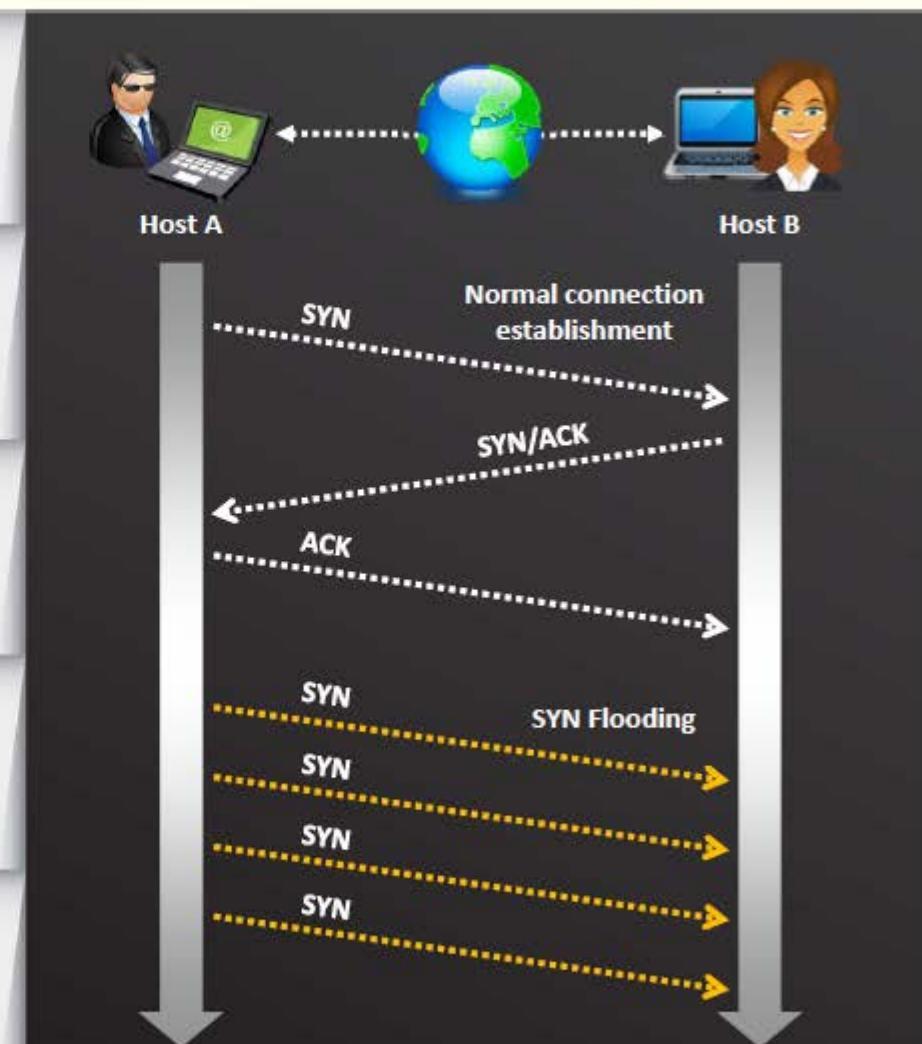
A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but **never replying** to the SYN/ACK

4

The victim's listen queue is **quickly filled up**

5

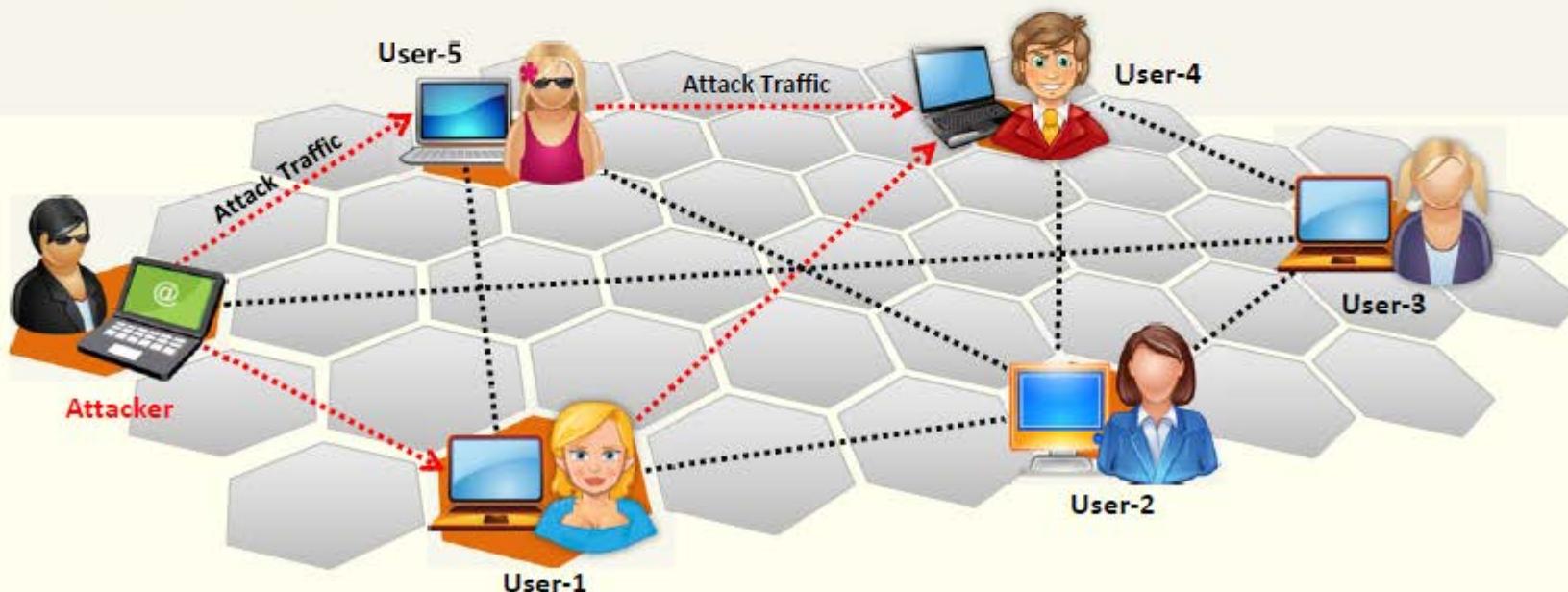
This ability of **holding up each incomplete connection for 75 seconds** can be cumulatively used as a Denial-of-Service attack



# Peer-to-Peer Attacks



- Using peer-to-peer attacks, attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website
- Attackers exploit flaws found in the network using DC++ (Direct Connect) protocol, that is used for sharing all types of files between instant messaging clients
- Using this method, attackers launch massive denial-of-service attacks and compromise websites



# Permanent Denial-of-Service Attack

CEH  
Certified Ethical Hacker

Permanent DoS, also known as **phashing**, refers to attacks that cause irreversible damage to system hardware

**Phashing**

Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

**Sabotage**

- This attack is carried out using a method known as "**bricking a system**"
- Using this method, attackers send **fraudulent hardware updates** to the victims

**Bricking a system**

**Process**



Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates

Attacker gets access to victim's computer



(Malicious code is executed)

# Permanent Denial-of-Service Attack

CEH  
Certified Ethical Hacker

Permanent DoS, also known as **phashing**, refers to attacks that cause irreversible damage to system hardware

**Phashing**

Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

**Sabotage**

- This attack is carried out using a method known as "**bricking a system**"
- Using this method, attackers send **fraudulent hardware updates** to the victims

**Bricking a system**

**Process**



Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates

Attacker gets access to victim's computer



(Malicious code is executed)

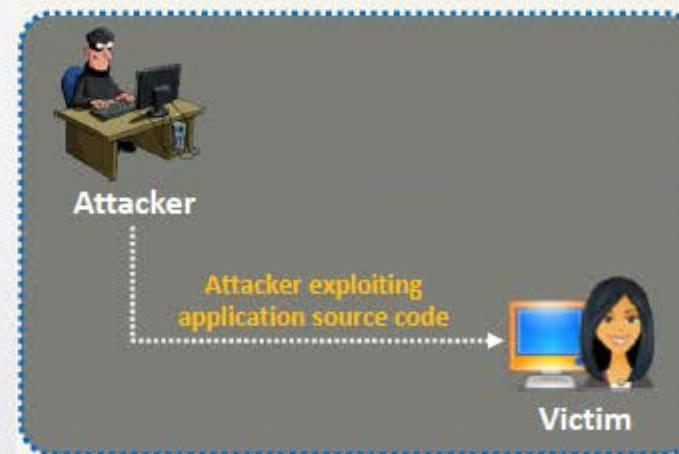
# Application-Level Flood Attacks

C|EH  
Certified Ethical Hacker

- Application-level flood attacks result in the **loss of services** of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more
- Using this attack, attackers **exploit weaknesses in programming source code** to prevent the application from processing legitimate requests

## Using application-level flood attacks, attackers attempts to:

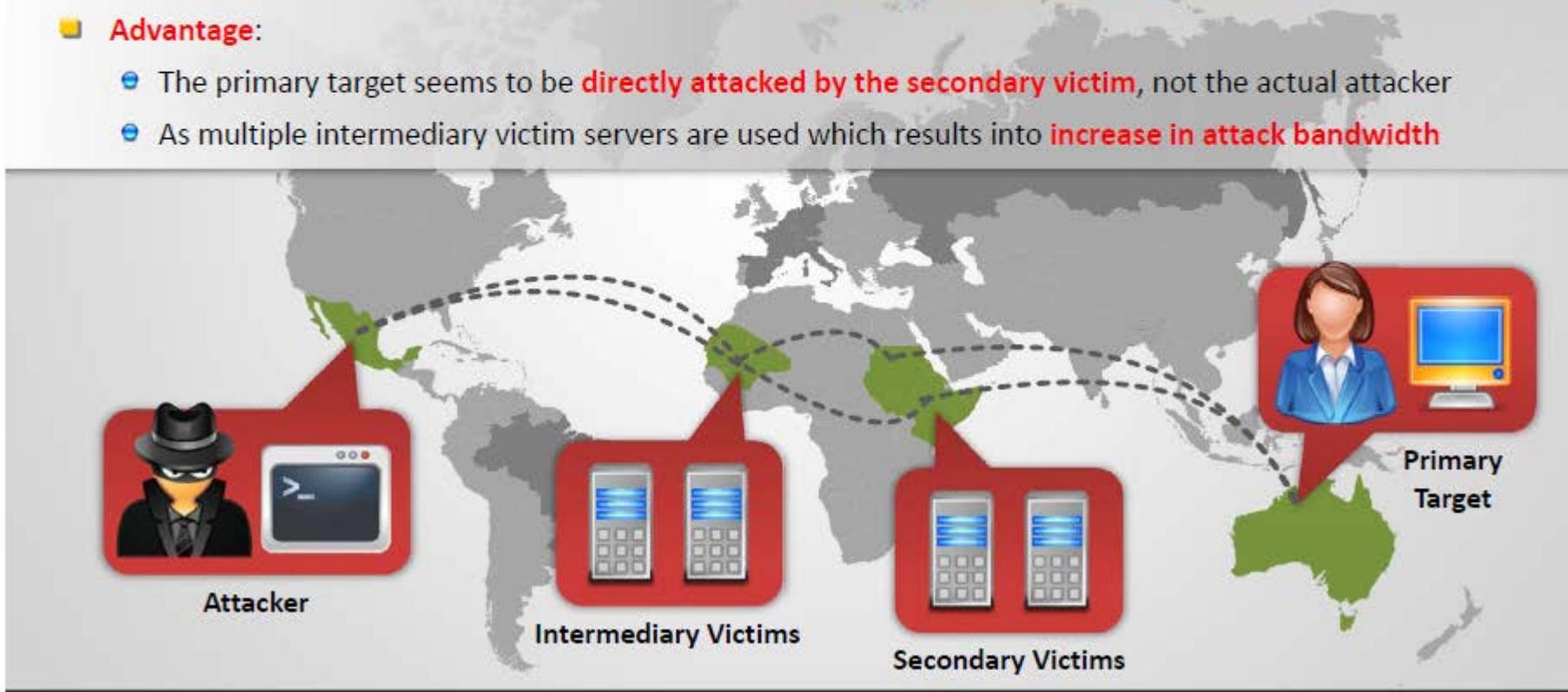
- Flood web applications to legitimate user traffic
- Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- Jam the application-database connection by crafting malicious SQL queries



# Distributed Reflection Denial of Service (DRDoS)

**C|EH**  
Certified Ethical Hacker

- A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the **use of multiple intermediary and secondary machines** that contribute to the actual DDoS attack against the target machine or application
- Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn **reflects the attack traffic to the target**
- **Advantage:**
  - The primary target seems to be **directly attacked by the secondary victim**, not the actual attacker
  - As multiple intermediary victim servers are used which results into **increase in attack bandwidth**



# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

**6 Countermeasures**

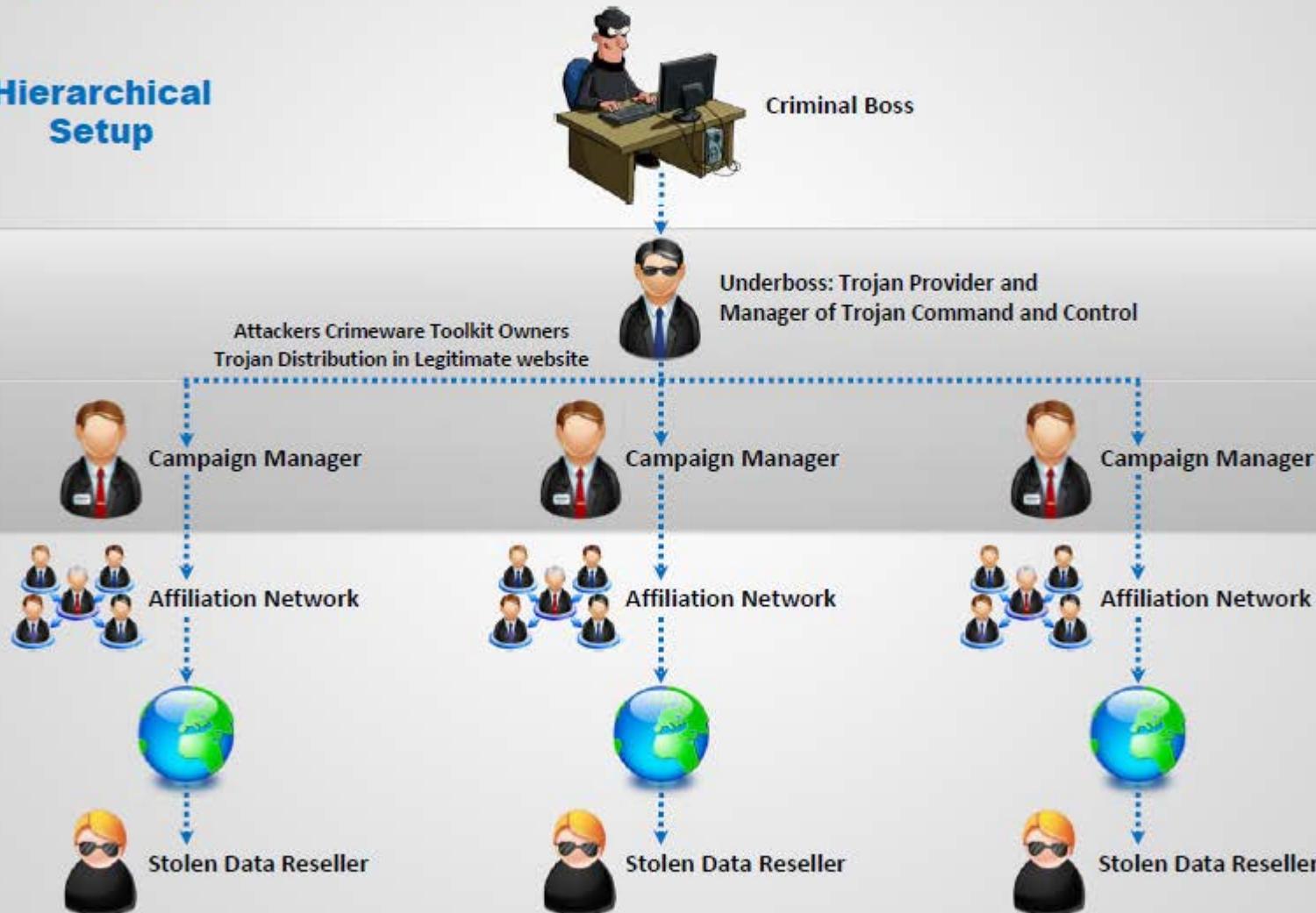
**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# Organized Cyber Crime: Organizational Chart

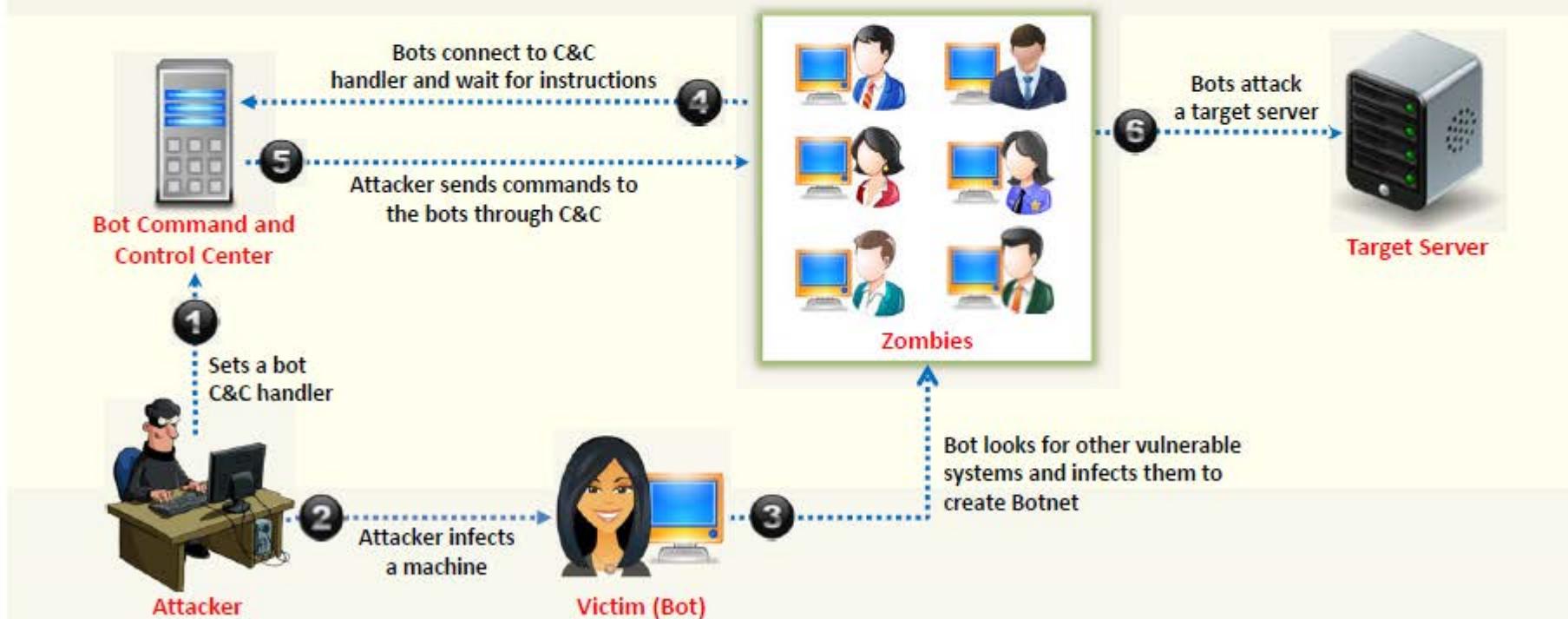
**CEH**  
Certified Ethical Hacker

## Hierarchical Setup



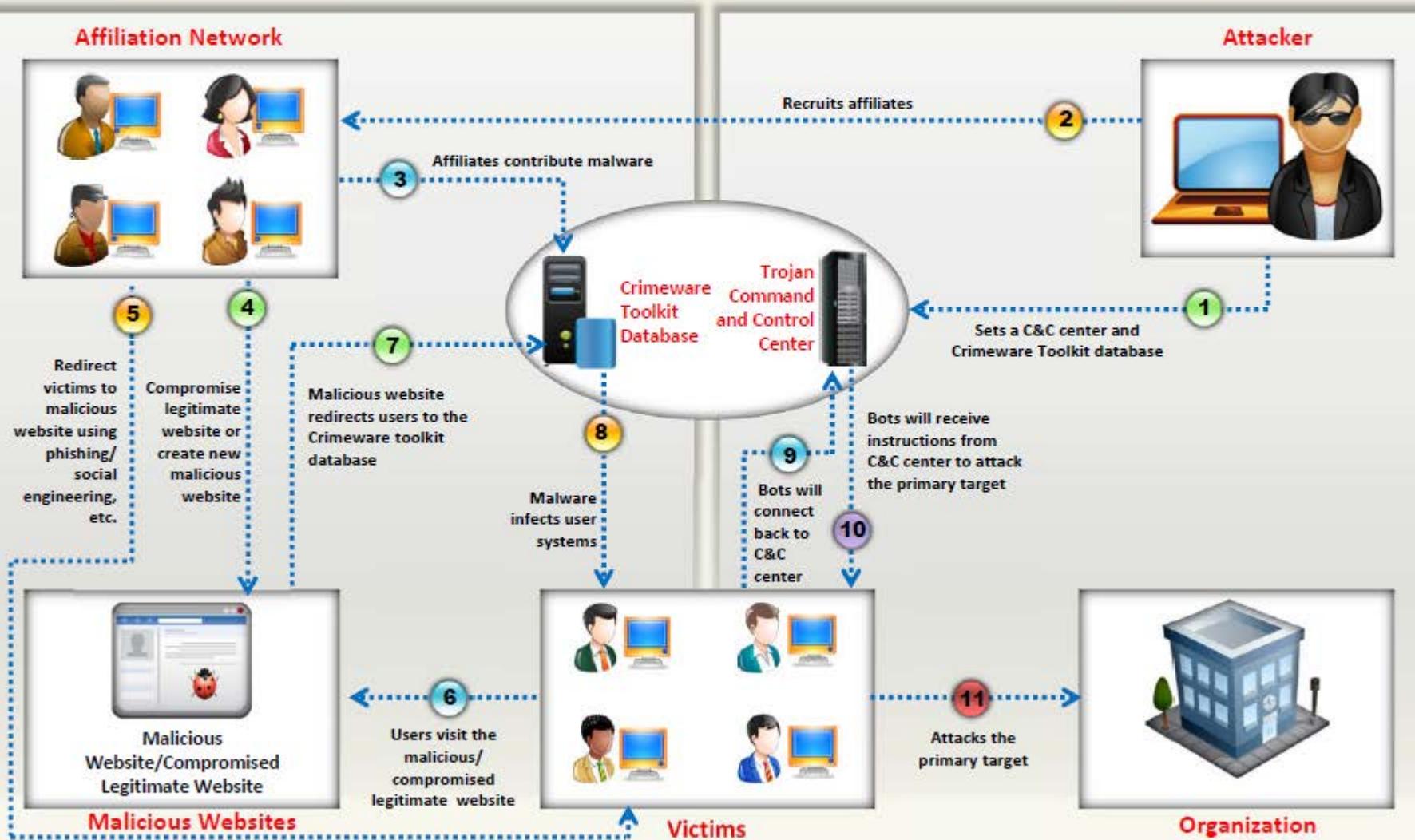
# Botnet

- 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 attacker to **launch denial-of-service attacks**



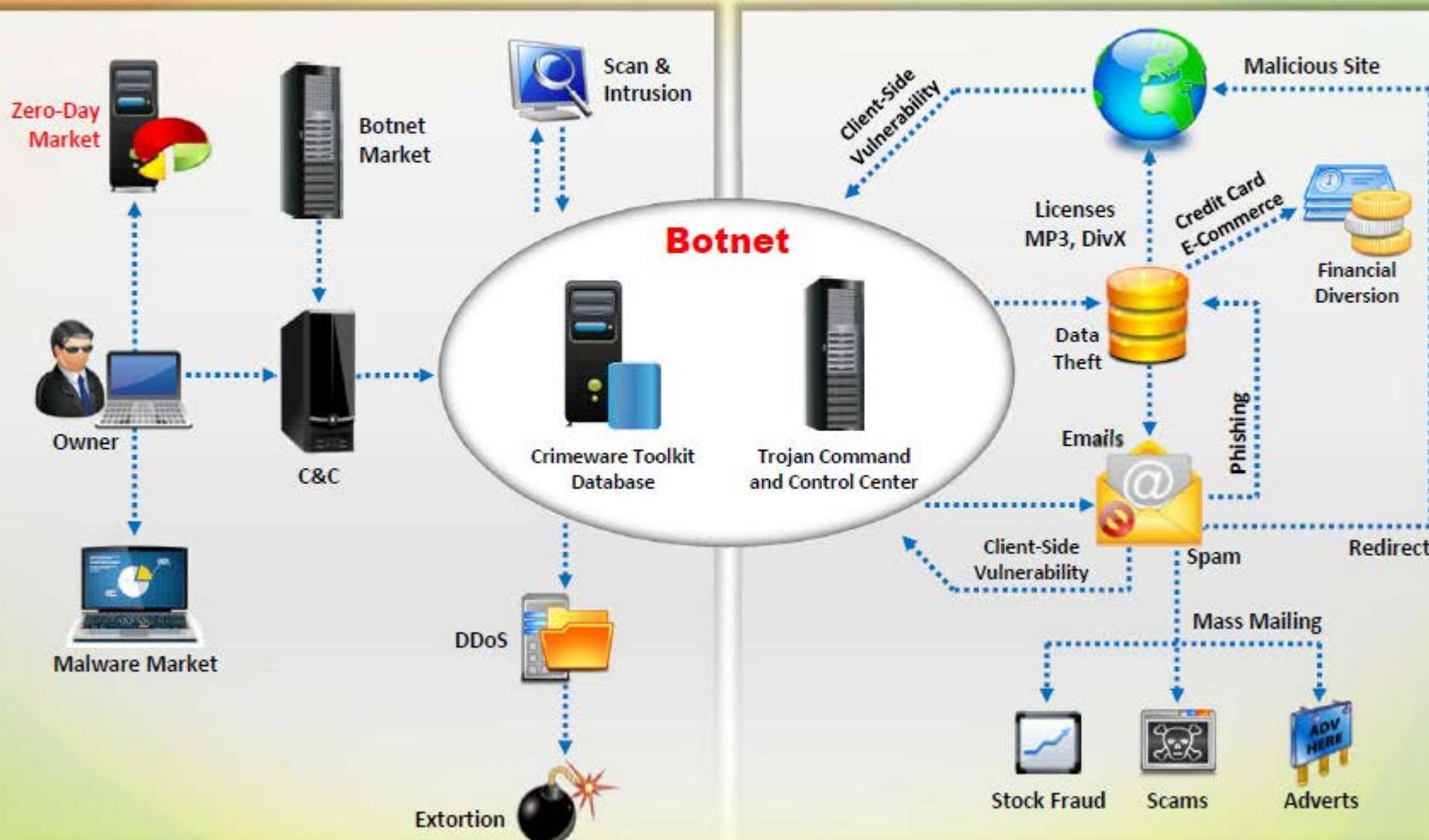
# A Typical Botnet Setup

CEH  
Certified Ethical Hacker



# Botnet Ecosystem

CEH  
Certified Ethical Hacker



# Scanning Methods for Finding Vulnerable Machines



## Random Scanning

The infected machine probes **IP addresses** randomly from **target network IP range** and checks for the vulnerability

## Hit-list Scanning

Attacker first collects list of possible **potentially vulnerable machines** and then perform scanning to find vulnerable machine

## Topological Scanning

It uses the **information obtained on infected machine** to find new vulnerable machines

## Local Subnet Scanning

The infected machine looks for the **new vulnerable machines in its own local network**

## Permutation Scanning

It uses **pseudorandom permutation list of IP addresses** to find new vulnerable machines

# How Malicious Code Propagates?

Attackers use three techniques to propagate malicious code to newly discovered vulnerable system

Attacker places **attack toolkit** on the central source and copy of the attack toolkit is transferred to the newly discovered vulnerable system

## Central Source Propagation



Attacker places **attack toolkit** on his/her system itself and copy of the attack toolkit is transferred to the newly discovered vulnerable system

## Autonomous Propagation

Attack toolkit is transferred at the time when the new vulnerable system is discovered



# Botnet Trojan: Blackshades NET

CEH  
Certified Ethical Hacker

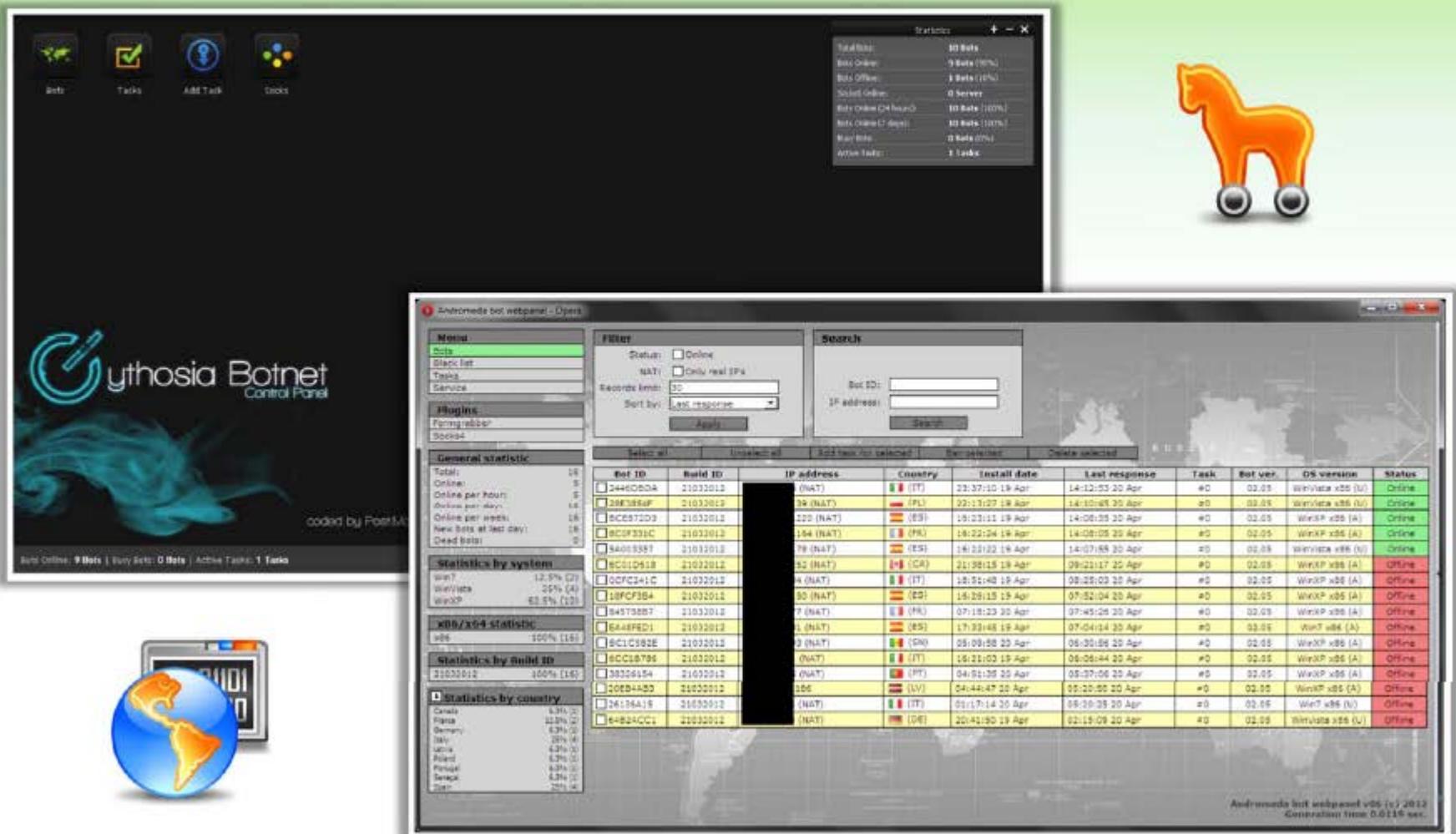
The screenshot shows the Blackshades NET software interface. On the left, there's a configuration panel for creating a bot. It includes fields for IP/DNS (set to 123.no-ip.info), Port (3080), Transfer port (4747), Server ID (Enter your Server ID), Keylog name (pa), Filename (Y9SP30613M.exe), Hide File (checked), Install path (App.Data), Sub folder (empty), Install mode (Install, Melt, Protect Process checked), Delay (No Delay), HKCU (Windows Defender, Startup checked), ActiveX (Generate), Mutex (ZMBAZN92GH), and Other (Infect USBs, Compress with UPX checked). Buttons for Save, Back, Example settings (highlighted in blue), and NET Crypter settings are at the bottom. Below this are tabs for Connections, Create Server, Create Station, Statistics, Settings, and Database.

On the right, there's an Information panel with checkboxes for Show thumbnail, Select All, Select Range, and Select Random. Overlaid on the main window is a smaller window titled "File Infector - 192.168.1.12.26 - NIGHTMARE". This window contains an ATTENTION! message: "Warning! Please take your time to read the following text for your own best. Your computer has basically been hijacked, and your private files stored on your computer has now been encrypted, which means that they are impossible to access, and can only be decrypted/restored by us". It also includes instructions: "Please settle X USD", "IBAN: XXXX 0040 0158 0000 0178 2101 XXXX", "SWIFT: XXXXX XXXXXX XXXXXXXX", "Account: IBAN505010100000225-1000", "Name: Somename Somelastname", and "City: Somecity". A Reference section notes: "Reference: Blackshades.key (WARNING: This must be included as a message or reference, otherwise your files will not be restored)". At the bottom of the overlay window are buttons for Help, Background color (white), Example, and Settings.

BlackShades NET has the ability to **create implant binaries** which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller

# Botnet Trojans: Cythosia Botnet and Andromeda Bot

C|EH  
Certified Ethical Hacker



The image shows two screenshots of botnet control panels. The left screenshot is for the 'Cythosia Botnet' and the right is for the 'Andromeda bot'. Both panels include a toolbar at the top with icons for Home, Tasks, Add Task, and Backs. The Cythosia panel has a sidebar with options like Status, Blocklist, Tasks, Service, Plugins, Firewall, and Socks4. It displays general statistics such as Total Bots (10 Bots), Bots Online (9 Bots 90%), Bots Offline (1 Bots 10%), and various log-in details. The Andromeda panel has a similar structure with a sidebar and a main table listing bot details. The table includes columns for Bot ID, Build ID, IP address, Country, Install date, Last response, Task, Bot ver., OS version, and Status. Most entries show the status as 'Online'. A large orange horse icon is positioned above the Andromeda panel.

**Cythosia Botnet Control Panel**

coded by PostM0d

**Andromeda bot webpanel - Open**

**General statistic**

Total	Online	Online per hour	Active per day	Online per week	New bots at last day	Dead total
10	9	1	1	1	0	0

**statistics by system**

win7	winxp	windows
12.9% (1)	25% (2)	62.5% (6)

**x86/x64 statistics**

x86	x64
100% (10)	0%

**Statistics by Build ID**

Build ID	Percentage
21032012	100% (10)

**D statistics by country**

Country	Percentage
Canada	6.3% (1)
Venezuela	11.3% (2)
Germany	6.3% (1)
Italy	28% (4)
Latvia	6.3% (1)
United States	6.3% (1)
United Kingdom	6.3% (1)
Senegal	6.3% (1)
Costa Rica	25% (4)

**Statistics**

Total Bots	10 Bots
Bots Online	9 Bots (90%)
Bots Offline	1 Bots (10%)
Social Online	0 Server
Bots Online CM (Avail)	10 Bots (100%)
Not Online CM (Avail)	10 Bots (100%)
Many Bots	0 Bots (0%)
Active Tasks	2 Tasks

**Andromeda bot webpanel v0.6 (v) 2013**  
Generation time: 0.0116 sec.

# Botnet Trojan: PlugBot

C|EH  
Certified Ethical Hacker



- PlugBot is a **hardware botnet project**
- It is a covert penetration testing device (bot) designed for **covert use during physical penetration tests**

Hello ADMIN | Last 5 Logs | Settings | Logout

**plugbot**

Dashboard >

Live Search... Go

Jobs

- Manage Jobs
- Add Job

Applications

- Manage Apps
- Add App

Bots

- Manage Bots
- Add Bot

Dashboard

Botnet Statistics

Quick View

PlugBot Statistics

Shown below are some quick stats on your botnet.

Statistics

- Bots: 2
- Jobs Pending: 0
- Jobs Completed: 0
- Check-Ins: 14636

© Copyright 2010-2011. A RedTeam Security Research Project



<http://theplugbot.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

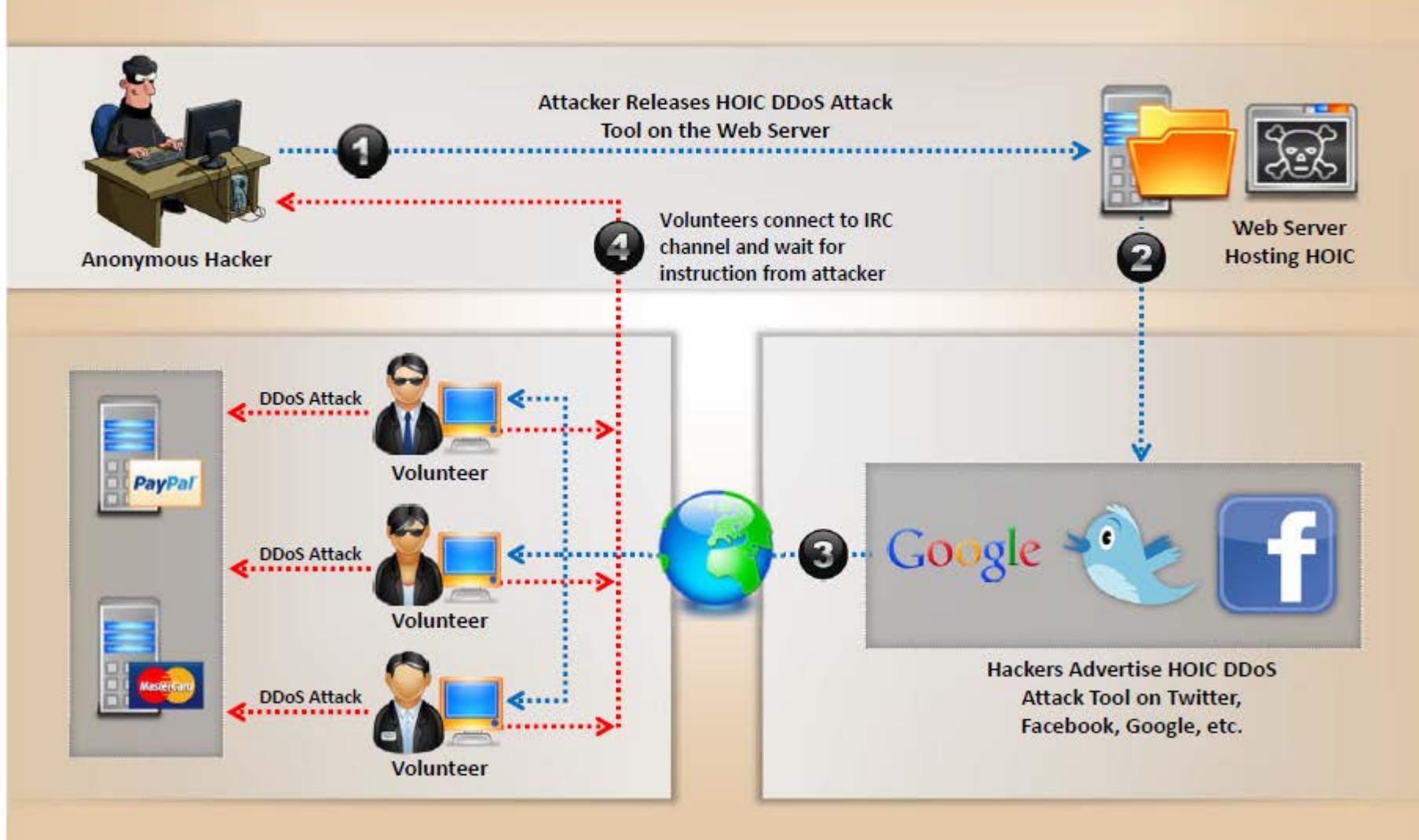
**6 Countermeasures**

**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# DDoS Attack

CEH  
Certified Ethical Hacker



# Hackers Advertise Links to Download Botnet

C|EH  
Certified Ethical Hacker

Guys how to fire!!! I want to be part of killing VISA

Click the above button. I understand the risk... better

Guys it's you!! FIRE@6fR3X... you guys watch so many movies... want to be part of a REVOLT! On!!!

it WILL make a difference. it's called 'not-reverence'. it's ok requiring us to do this job. I know it won't be a tea-pie what happens to VISA, we are not bowing to senator JOH while your freedoms are taken away.

On my god the government taking my freedom away and Visa is in the out! They want to control all of us...

It's like this service is purposeless. like why

Malware warning - MicroBlogBuzz.com

Post Picks: Don Cherry and the Link(s) - billy News and Comment

Operation Payback Setup Guide

#Wikileaks - Today Tweet Search

My App: Twitter Timeline - MuBook.com

Tweet It - What's Trending in France?

20 people are saying...

tanzmax@twitter RT @raimondiand: TARGET: [HTTP://WWW.TWITTER.COM](http://WWW.TWITTER.COM): FIRE FIRE FIRE!!! WEAPONS [HTTP://BIT.LY/E6F.R3X](http://bit.ly/e6fR3X) :: SET YOUR LOIC TO irc.anonops.net :: #PAYBACK #WIKILEAKS #anonops Shared about 5 hours ago.

chelechimak@twitter RT @Irvamondiand: RT @Anon\_operators: NEXT TARGET: [HTTP://WWW.VISA.COM](http://WWW.VISA.COM) | TR:30 MINS. GET YOUR WEAPONS READY [HTTP://BIT.LY/E6F.R3X](http://bit.ly/e6fR3X) #ddos #wikileaks #payback Shared about 6 hours ago.

keithpo@twitter RT @Anon\_Operations: CURRENT TARGET: [HTTP://WWW.VISA.COM](http://WWW.VISA.COM) :: WEAPONS [HTTP://BIT.LY/E6F.R3X](http://bit.ly/e6fR3X) :: SET YOUR LOIC TO --> irc.anonops.net & FIRE FIRE FIRE!!! #WIKILEAKS #DDOS Shared about 7 hours ago.

davv21@twitter RT @La\_Begge: ST SABES DE CYBERSHIT, ATACA DESDE ACÁ: [HTTP://PASTEBIN1.COM/VIEW/1C8133U.HTML](http://pastebin1.com/view/1cB133u.html) #Payback #Wikileaks (@kno\_z live on [HTTP://JWTEAM.COM/20FA](http://jwteam.com/20fa)) Shared about 7 hours ago.

Justin\_Hop@twitter RT @Anon\_Operations: CURRENT TARGET: [HTTP://WWW.VISA.COM](http://WWW.VISA.COM) :: WEAPONS [HTTP://BIT.LY/E6F.R3X](http://bit.ly/e6fR3X) :: SET YOUR LOIC TO --> irc.anonops.net & FIRE FIRE FIRE!!! #WIKILEAKS #DDOS Shared about 7 hours ago.

# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

**6 Countermeasures**

**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit



The Pandora DDoS Bot Toolkit is an updated variant of the **Dirt Jumper DDoS toolkit**

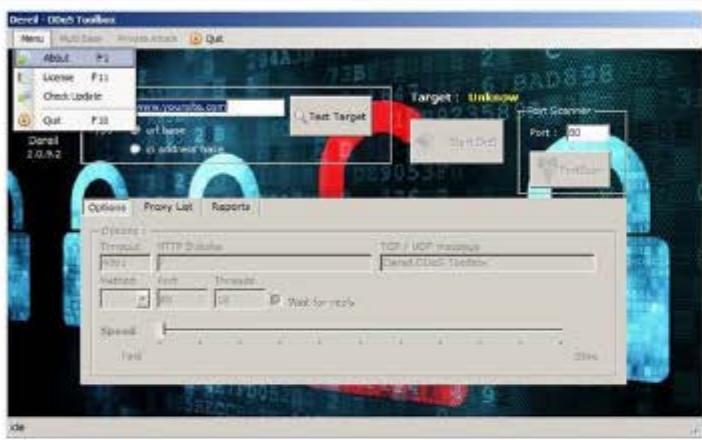
It offers five distributed denial of service (**DDoS**) attack modes

**It generates five attack types:**

- HTTP min
- HTTP download
- HTTP Combo
- Socket Connect
- Max Flood



# DoS and DDoS Attack Tools: Dereil and HOIC



<http://sourceforge.net>

## Dereil

Dereil is professional (DDoS)  
Tools with modern patterns  
for attack via **TCP, UDP**, and  
**HTTP protocols**



## HOIC



HOIC makes a DDoS attacks  
to **any IP address**, with a  
user selected port and a  
user selected protocol



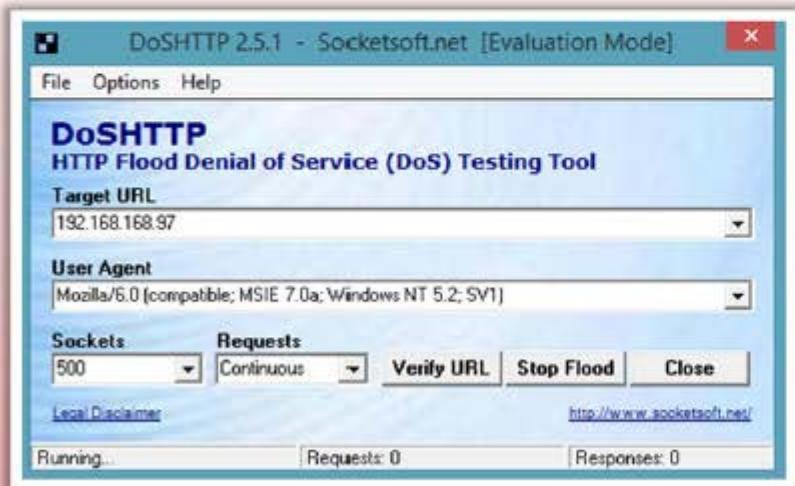
<http://sourceforge.net>

# DoS and DDoS Attack Tools: DoS HTTP and BanglaDos



## DoS HTTP

- DoSHTTP is **HTTP Flood** Denial of Service (DoS) Testing Tool for Windows
- It includes **URL verification**, **HTTP redirection**, port designation, performance monitoring and enhanced reporting
- It uses **multiple asynchronous sockets** to perform an effective HTTP Flood



<http://socketsoft.net>

## BanglaDos



<http://sourceforge.net>

# DoS and DDoS Attack Tools

**CEH**  
Certified Ethical Hacker



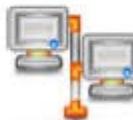
**Tor's Hammer**

<http://packetstormsecurity.com>



**Anonymous-DoS**

<http://sourceforge.net>



**DAVOSET**

<http://packetstormsecurity.com>



**PyLoris**

<http://sourceforge.net>



**LOIC**

<http://sourceforge.net>



**Moihack Port-Flooder**

<http://sourceforge.net>



**DDOSIM**

<http://sourceforge.net>



**HULK**

<http://www.sectorix.com>



**R-U-Dead-Yet**

<https://code.google.com>



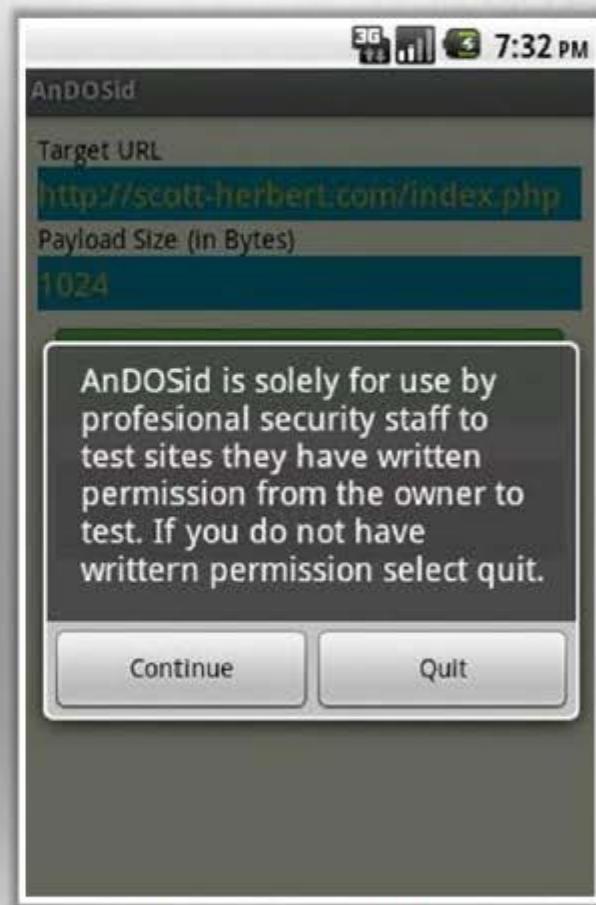
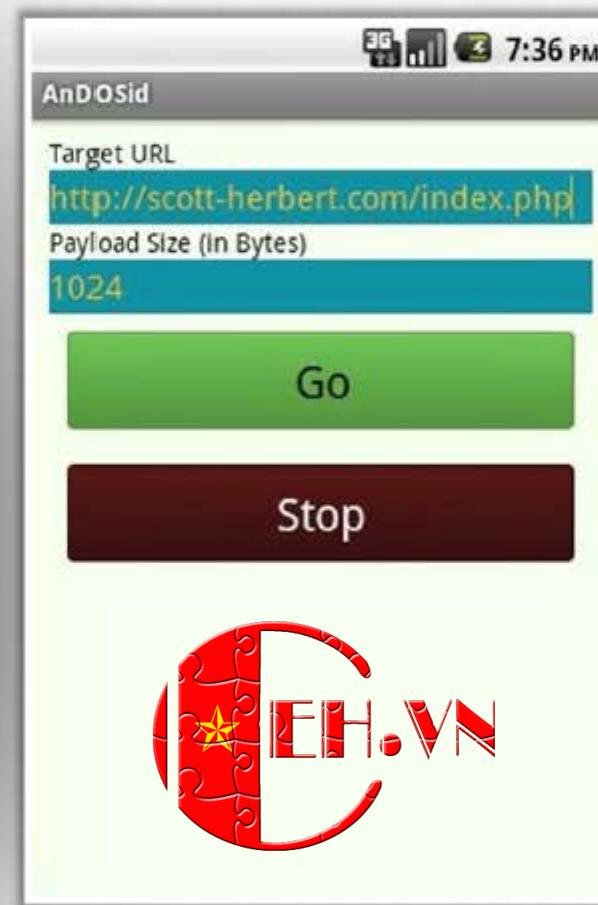
**GoldenEye HTTP Denial Of Service Tool**

<http://packetstormsecurity.com>

# DoS and DDoS Attack Tool for Mobile: AnDOSid



- AnDOSid allows attacker to simulate a **DOS attack** (A http post flood attack to be exact) and **DDoS attack on a web server** from mobile phones

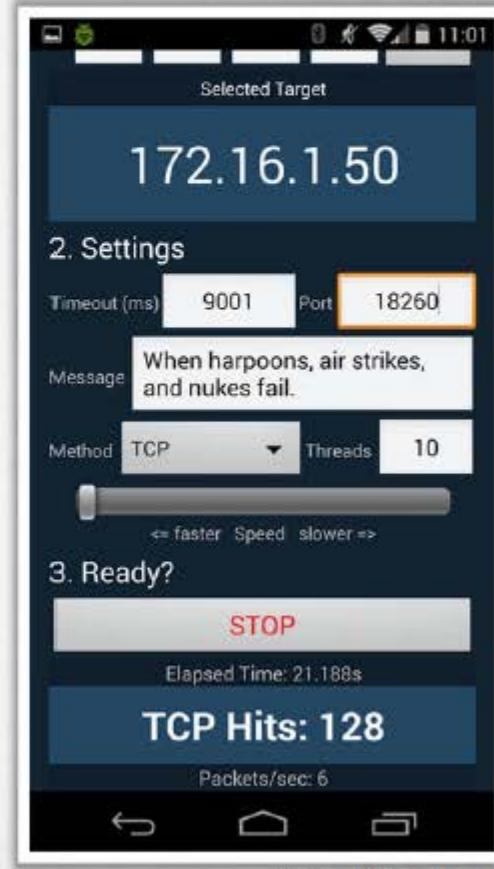
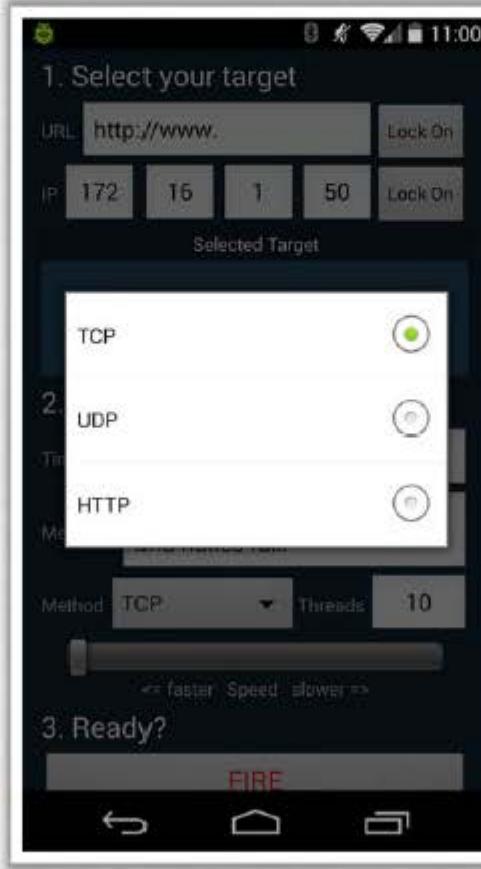
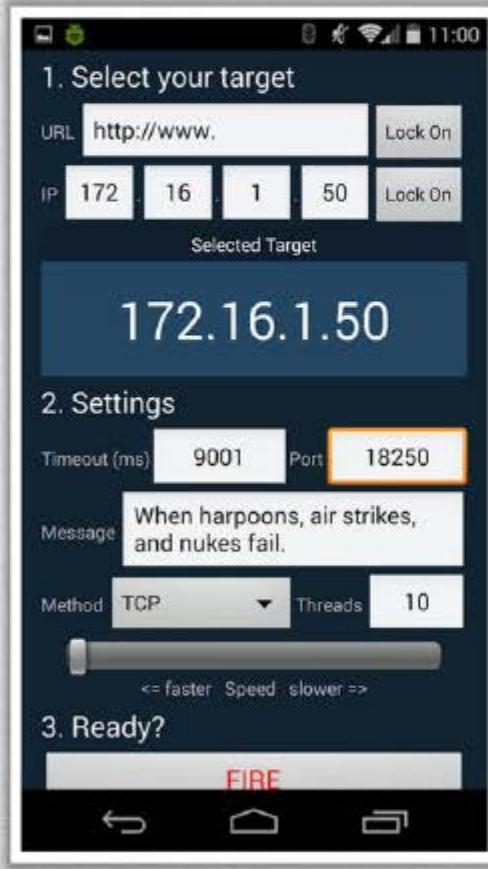


<http://andosid.android.informer.com>

# DoS and DDoS Attack Tool for Mobile: Low Orbit Ion Cannon (LOIC)



- Android version of Low Orbit Ion Cannon (LOIC) software is used for **flooding packets** which allows attacker to **perform DDoS attack** on target organization



<https://github.com>

# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

**6 Countermeasures**

**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# Detection Techniques

CEH  
Certified Ethical Hacker

01

Activity Profiling



02

Changepoint Detection



03

Wavelet-based Signal Analysis



All detection techniques define an attack as an **abnormal and noticeable deviation** from a threshold of normal network traffic statistics

# Activity Profiling

1

An attack is indicated by:

- An increase in activity levels among the **network flow clusters**
- An increase in the overall number of **distinct clusters** (DDoS attack)



2

Activity profile is done based on the **average packet rate** for a network flow, which consists of consecutive packets with similar packet fields

3

Activity profile is obtained by monitoring the **network packet's header information**



# Wavelet-based Signal Analysis

C|EH  
Certified Ethical Hacker



Wavelet analysis describes an input signal in terms of **spectral components**



Wavelets provide for concurrent **time** and **frequency** description



Analyzing each spectral window's energy determines the presence of **anomalies**



Signal analysis determines the time at which certain **frequency components** are present

# Sequential Change-Point Detection



## Isolate Traffic

Change-point detection algorithms **isolate changes in network traffic statistics** caused by attacks



## Filter Traffic

The algorithms filter the **target traffic data** by address, port, or protocol and store the resultant flow as a time series



## Identify Attack

Sequential change-point detection technique uses Cusum algorithm to identify and locate the **DoS attacks**; the algorithm calculates deviations in the actual versus expected local average in the traffic time series



## Identify Scan Activity

This technique can also be used to identify the typical **scanning activities of the network worms**



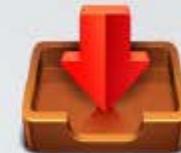
# DoS/DDoS Countermeasure Strategies



## Absorbing the Attack

01

- Use additional capacity to absorb attack; it requires preplanning
- It requires additional resources



## Degrading Services



02

- Identify critical services and stop non critical services

03

## Shutting Down the Services

- Shut down all the services until the attack has subsided



# DDoS Attack Countermeasures

**CEH**  
Certified Ethical Hacker

01

**Protect Secondary Victims**



02

**Neutralize Handlers**



03

**Prevent Potential Attacks**



04

**Deflect Attacks**



05

**Mitigate Attacks**



06

**Post-attack Forensics**



# DoS/DDoS Countermeasures: Protect Secondary Victims



Install **anti-virus** and **anti-Trojan** software and keep these up-to-date



Increase **awareness of security issues** and prevention techniques in all Internet users



**Disable unnecessary services**, uninstall unused applications, and scan all the files received from external sources



Properly configure and regularly update the **built-in defensive mechanisms** in the core hardware and software of the systems

# DoS/DDoS Countermeasures: Detect and Neutralize Handlers



## Network Traffic Analysis

Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents in order to **identify the network nodes** that might be infected by the handlers



## Neutralize Botnet Handlers

There are usually few **DDoS handlers deployed** as compared to the number of agents. Neutralizing a few handlers can possibly **render multiple agents** useless, thus thwarting DDoS attacks



## Spoofed Source Address

There is a decent probability that the spoofed source address of DDoS attack packets will not represent a **valid source address of the definite sub-network**

# DoS/DDoS Countermeasures: Detect Potential Attacks

CEH  
Certified Ethical Hacker

- Scanning the **packet headers** of IP packets leaving a network
- Egress filtering ensures that **unauthorized or malicious traffic** never leaves the internal network

## Egress Filtering

- Protects from **flooding attacks** which originate from the valid prefixes (IP addresses)
- It enables the originator to be traced to its **true source**



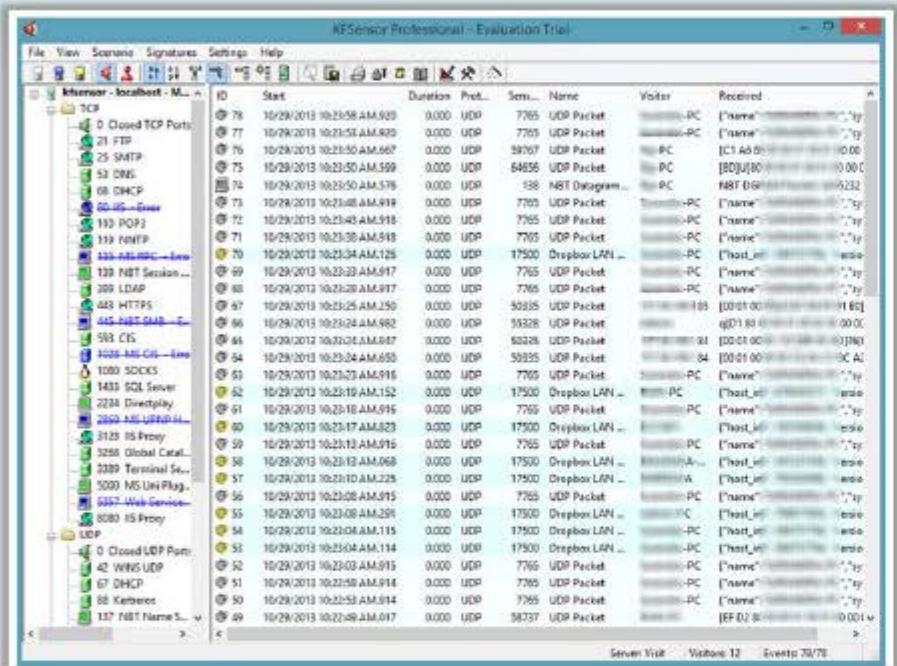
## Ingress Filtering

- Configuring TCP Intercept **prevents DoS attacks** by intercepting and validating the TCP connection requests

## TCP Intercept



# DoS/DDoS Countermeasures: Deflect Attacks



<http://www.keyfocus.net>



Systems that are set up with limited security, also known as Honeypots,  
**act as an enticement** for an attacker



Honeypots serve as a means for  
**gaining information** about attackers,  
attack techniques and tools by storing  
a record of the system activities



Use **defense-in-depth** approach with  
IPSecs at different network points to  
divert suspicious DoS traffic to several  
honeypots



# DoS/DDoS Countermeasures: Mitigate Attacks

C|EH  
Certified Ethical Hacker



## Load Balancing

1

Increase bandwidth on **critical connections** to absorb additional traffic generated by an attack

2

Replicate servers to provide additional **failsafe** protection

3

Balance load on each server in a multiple-server architecture to **mitigates DDoS** attack

1

Set routers to access a server with a logic to throttle incoming traffic levels that are safe for the server

2

Throttling helps in preventing **damage to servers** by controlling the DoS traffic

3

Can be extended to throttle DDoS attack traffic and **allow legitimate user traffic** for better results

## Throttling



# Post-Attack Forensics

CEH  
Certified Ethical Hacker

1



DDoS attack traffic patterns can help the network administrators to develop **new filtering techniques** for preventing the attack traffic from entering or leaving the networks

2



Analyze router, firewall, and **IDS logs** to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and **law enforcement** agencies

3



**Traffic pattern analysis:** Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic

4



Using these characteristics, the result of traffic pattern analysis can be used for updating **load-balancing** and **throttling** countermeasures

# Techniques to Defend against Botnets



## RFC 3704 Filtering

Any traffic coming from unused or reserved IP addresses is bogus and **should be filtered at the ISP** before it enters the Internet link



## Cisco IPS Source IP Reputation Filtering

Reputation services help in determining if an **IP or service is a source of threat or not**, Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic

## Black Hole Filtering

Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient

Black hole filtering refers to **discarding packets at the routing level**

## DDoS Prevention Offerings from ISP or DDoS Service

**Enable IP Source Guard** (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets

# DoS/DDoS Countermeasures



Use **strong encryption mechanisms** such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping



Ensure that the software and protocols are **up-to-date** and scan the machines thoroughly to detect any **anomalous behavior**



Disable **unused** and **insecure services**



Block all **inbound packets** originating from the service ports to block the traffic from reflection servers



Update **kernel** to the latest release



Prevent the transmission of the **fraudulently addressed packets** at ISP level



Implement **cognitive radios** in the physical layer to handle the jamming and scrambling attacks

# DoS/DDoS Countermeasures

(Cont'd)



Configure the firewall to deny **external ICMP traffic access**



Secure the **remote administration** and **connectivity testing**



Perform the thorough **input validation**



Data processed by the attacker should be **stopped from being executed**



Prevent use of **unnecessary functions** such as gets, strcpy etc.



Prevent the **return addresses** from being overwritten

# DoS/DDoS Protection at ISP Level

C|EH  
Certified Ethical Hacker



Most ISPs simply blocks all the requests during a **DDoS attack**, **denying even the legitimate traffic** from accessing the service



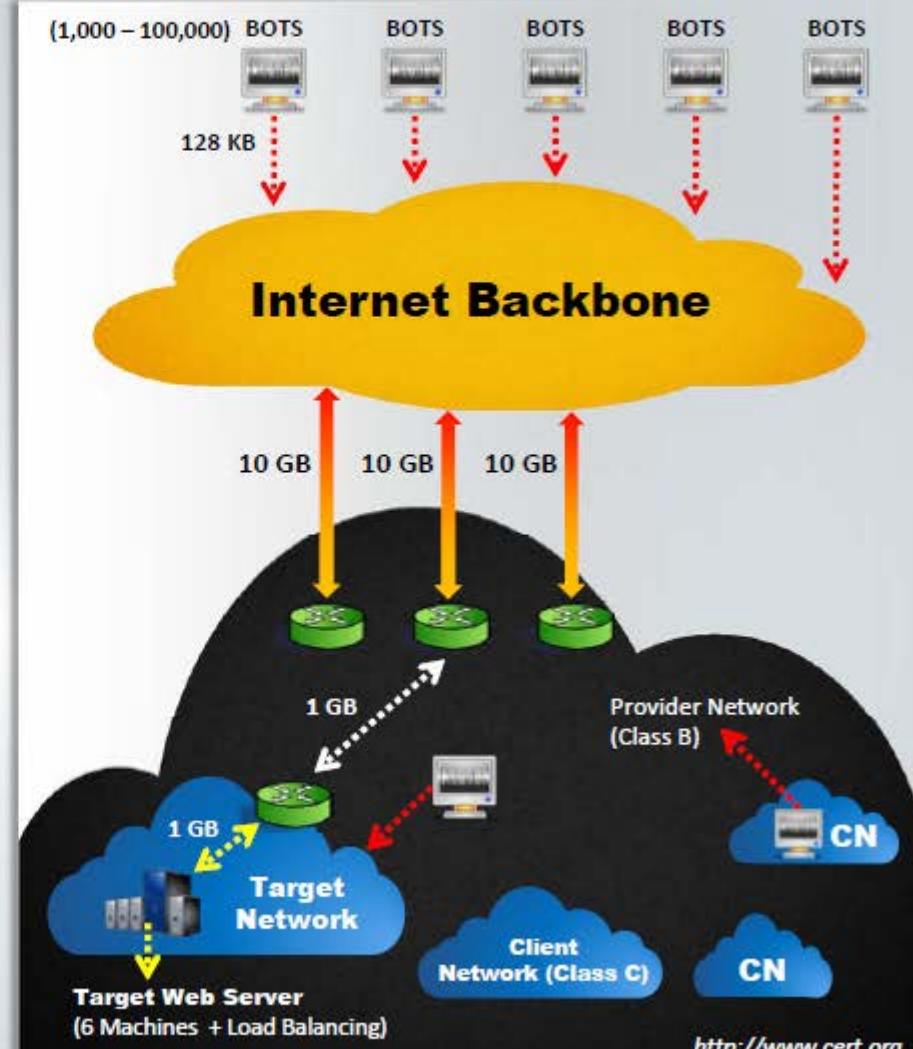
ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become **saturated by the attack**



Attack traffic is **redirected to the ISP** during the attack to be filtered and sent back



Administrators can **request ISPs** to block the original affected IP and move their site to another IP after performing DNS propagation



# Enabling TCP Intercept on Cisco IOS Software



To enable TCP intercept, use these commands in global configuration mode:

Step	Command	Purpose
1	access-list access-list-number {deny   permit} tcp any destination destination-wildcard	Define an IP extended access list
2	ip tcp Intercept list <i>access-list-number</i>	Enable TCP Intercept



TCP intercept can operate in either **active intercept** mode or **passive watch** mode. The default is intercept mode

The command to set the TCP intercept mode in **global configuration** mode:

Command	Purpose
ip tcp intercept mode {intercept   watch}	Set the TCP intercept mode



<http://www.cisco.com>

# Advanced DDoS Protection Appliances



FortiDDoS-300A



<http://www.fortinet.com>

DDoS Protector



<http://www.checkpoint.com>

Cisco Guard XT 5650



<http://www.cisco.com>

Arbor Pravail: Availability Protection System



<http://www.arbornetworks.com>

# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

**6 Countermeasures**

**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# DoS/DDoS Protection Tool: FortGuard Anti-DDoS Firewall 2014



FortGuard Anti-DDoS Firewall provides a fundamentally superior approach to mitigating DDoS attacks, with a design that focuses on **passing legitimate traffic rather than discarding attack traffic**



## Features:

- Protection against SYN, TCP Flooding and other types of DDoS attacks
- Attack packets filtering; UDP/ICMP/IGMP packets rate management
- Protection against arp spoofing



# DoS/DDoS Protection Tools

**CEH**  
Certified Ethical Hacker



**NetFlow Analyzer**

<http://www.manageengine.com>



**SDL Regex Fuzzer**

<http://www.microsoft.com>



**WANGuard Sensor**

<http://www.andrisoft.com>



**NetScaler Application Firewall**

<http://www.citrix.com>



**Incapsula**

<http://www.incapsula.com>



**FortiDDoS**

<http://www.fortinet.com>



**DefensePro**

<http://www.radware.com>



**DOSarrest**

<http://www.dosarrest.com>



**Anti DDoS Guardian**

<http://www.beethink.com>



**DDoSDefend**

<http://ddosdefend.com>

# Module Flow



**1 DoS/DDoS Concepts**

**2 DoS/DDoS Attack Techniques**

**3 Botnets**

**4 DDoS Case Study**

**5 DoS/DDoS Attack Tools**

**6 Countermeasures**

**7 DoS/DDoS Protection Tools**

**8 DoS/DDoS Penetration Testing**

# Denial-of-Service (DoS) Attack

## Penetration Testing

**CEH**  
Certified Ethical Hacker

1



DoS attack should be incorporated into Pen testing plans to find out if the **network server** is susceptible to DoS attacks

2



DoS Pen Testing **determines minimum thresholds for DoS attacks on a system**, but the tester cannot ensure that the system is resistant to DoS attacks

3



The pen tester **floods the target network with traffic**, similar to hundreds of people repeatedly requesting the service in order to check the system stability

4



Pen testing results will help the administrators to **determine and adopt suitable network perimeter security controls** such as load balancer, IDS, IPS, Firewalls, etc.

# Denial-of-Service (DoS) Attack

## Penetration Testing (Cont'd)



Define Objective

START

Test for heavy loads on the server

Check for DoS vulnerable systems

Run SYN attack on the server

Run port flooding attacks on the server



Document all the Findings

Flood the website forms and guestbook with bogus entries

Run email bomber on the email servers

- Test the web server using automated tools such as **Webserver Stress Tool** and **JMeter** for load capacity, server-side performance, locks, and other scalability issues
- Scan the network using automated tools such as **Nmap**, **GFI LanGuard**, and **Nessus** to discover any systems that are vulnerable to DoS attacks
- Flood the target with connection request packets using tools such as **Dirt Jumper DDoS Toolkit**, **Dereil**, **HOIC**, and **DoS HTTP**
- Use a port flooding attack to flood the port and increase the CPU usage by maintaining all the connection requests on the ports under blockade. Use tools **LOIC** and **Mohack Port Flooder** to automate a port flooding attack
- Use tools **Mail Bomber** to send a large number of emails to a target mail server
- Fill the forms with **arbitrary** and **lengthy** entries



# Module Summary



- ❑ Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users
- ❑ A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system
- ❑ Attacker uses various techniques to carry out DoS/DDoS attacks on the target but these attacks are basically categorized into; volumetric attacks, fragmentation attacks, TCP state-exhaustion attacks, and application layer attacks
- ❑ There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, like a major corporation that offers criminal services
- ❑ A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks
- ❑ Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
- ❑ The pen tester floods the target network with traffic, similar to hundreds of people repeatedly requesting the service in order to check the system stability