# Denial-of-Service

## Module 09

Unmask the Invisible Hacker.

# Module Objectives

- 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

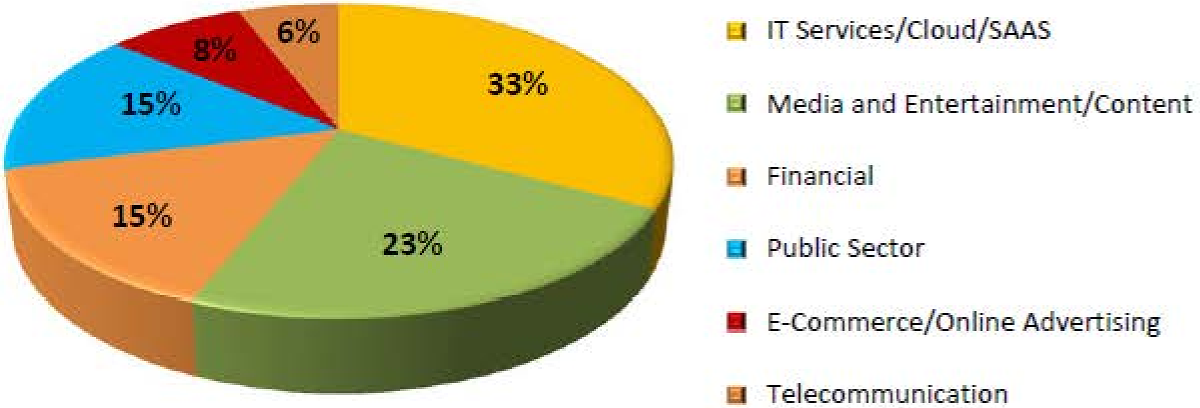
1. DoS/DDoS Concepts
2. DoS/DDoS Attack Techniques
3. Botnets
4. DDoS Case Study
5. DoS/DDoS Attack Tools
6. Countermeasures
7. DoS/DDoS Protection Tools
8. DoS/DDoS Penetration Testing

# DDoS Attack Trends

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

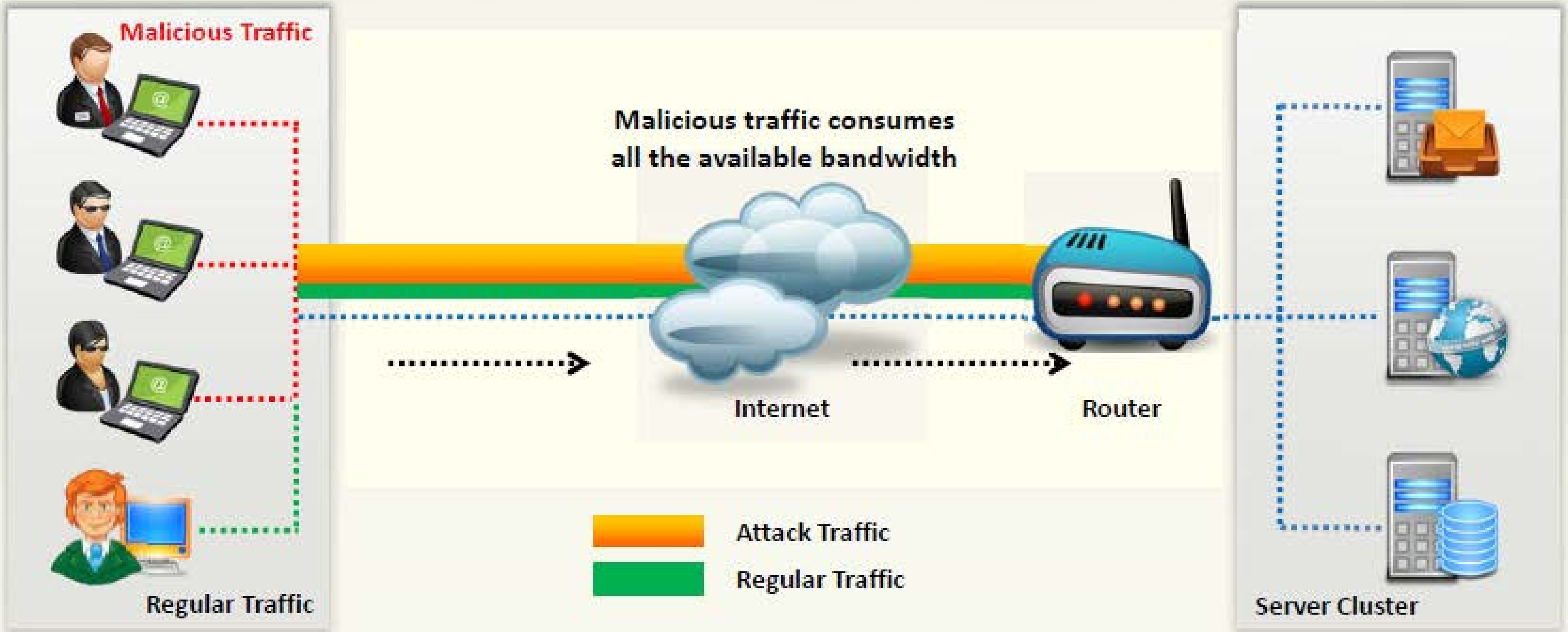
Mitigations By Industry Vertical - Q4 2014



*https://www.verisigninc.com*

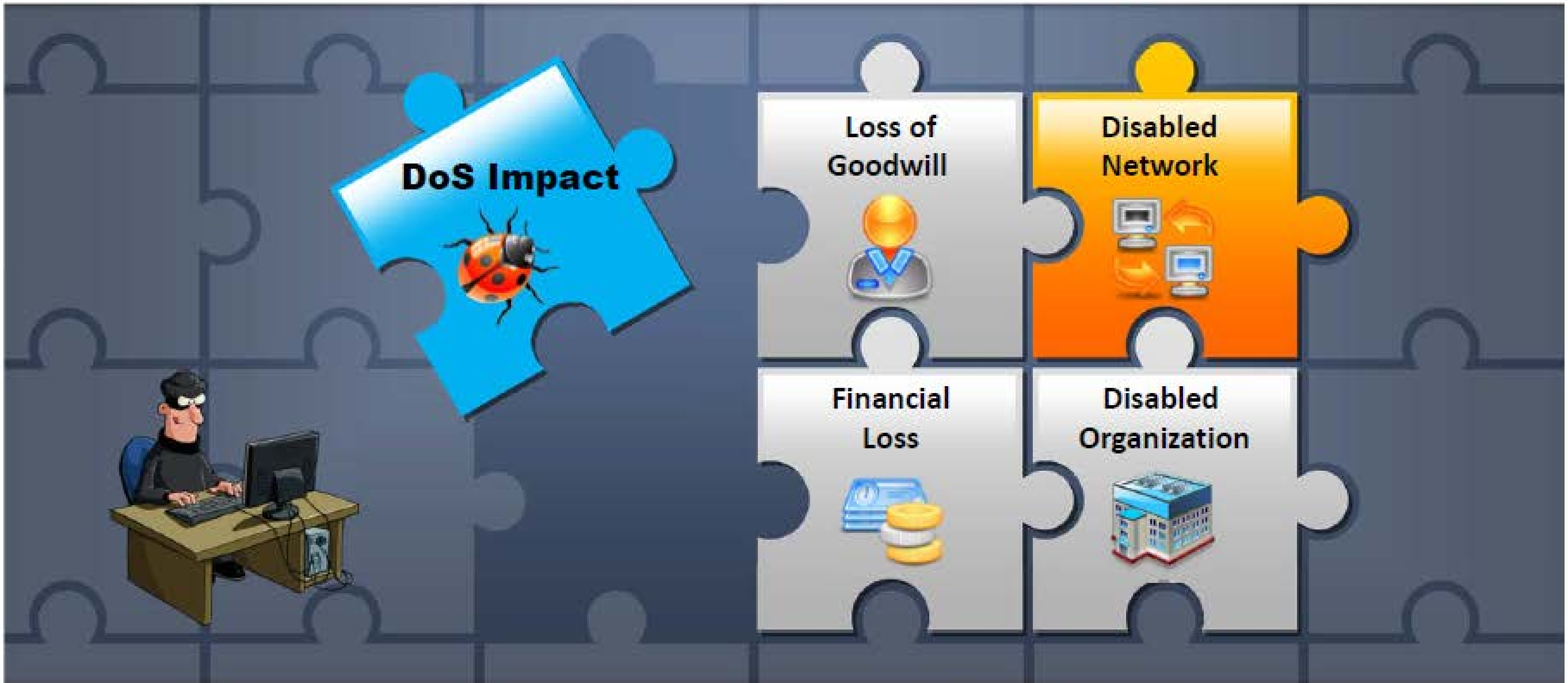
# What is a Denial-of-Service Attack?

- 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**

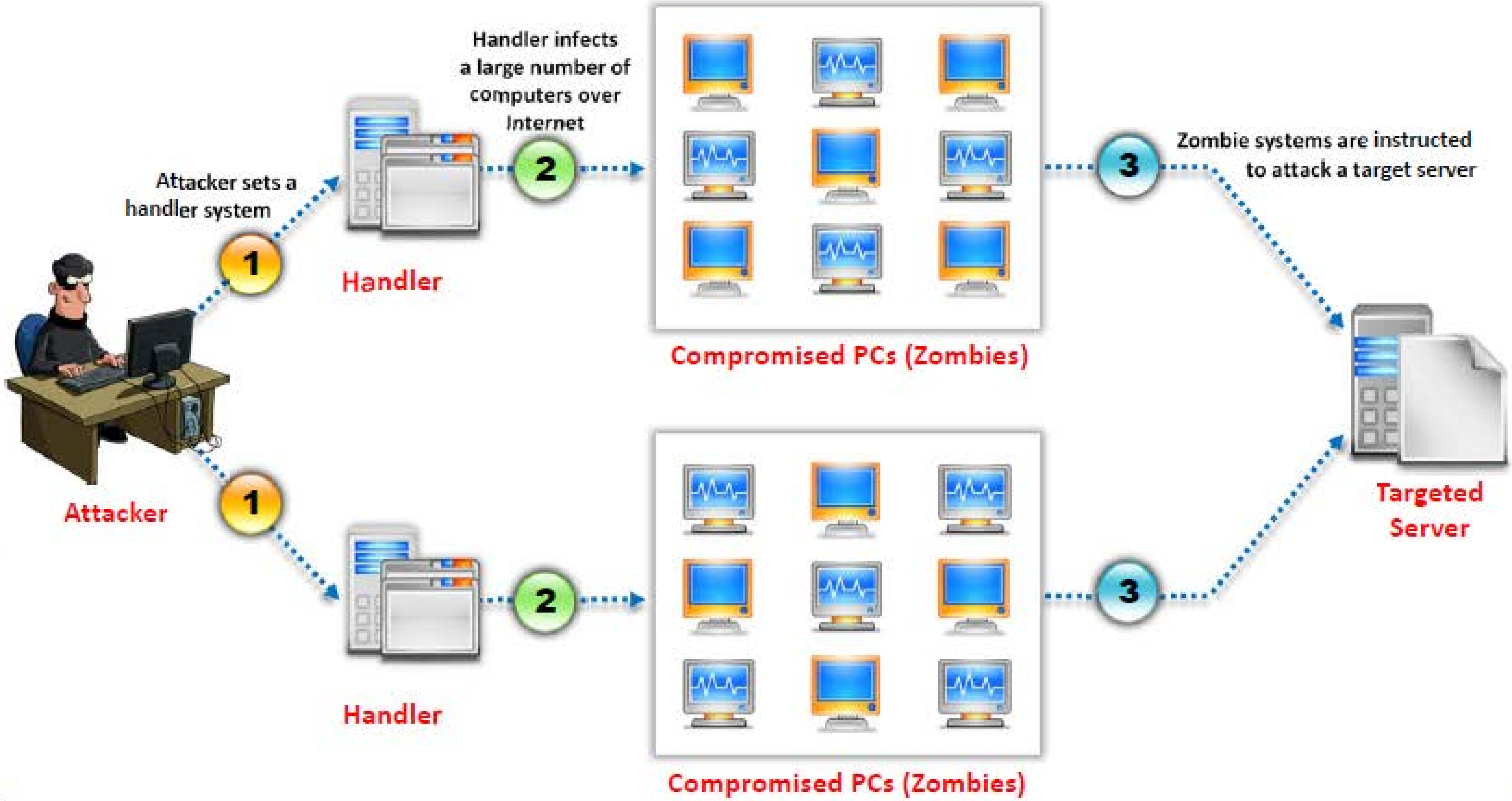


# What are Distributed Denial of Service Attacks?

- 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


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

# 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

### 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

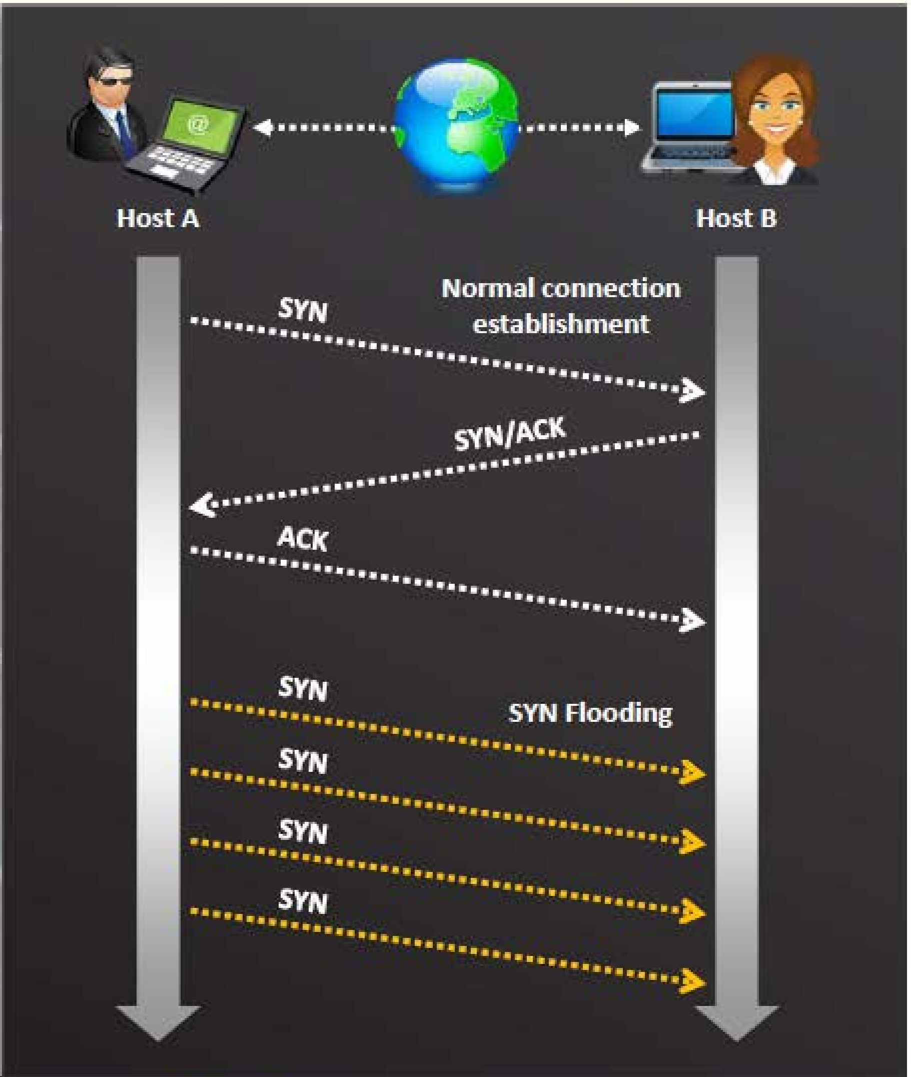
1 SYN Flooding takes advantage of a flaw in how most hosts implement the TCP **three-way handshake**

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

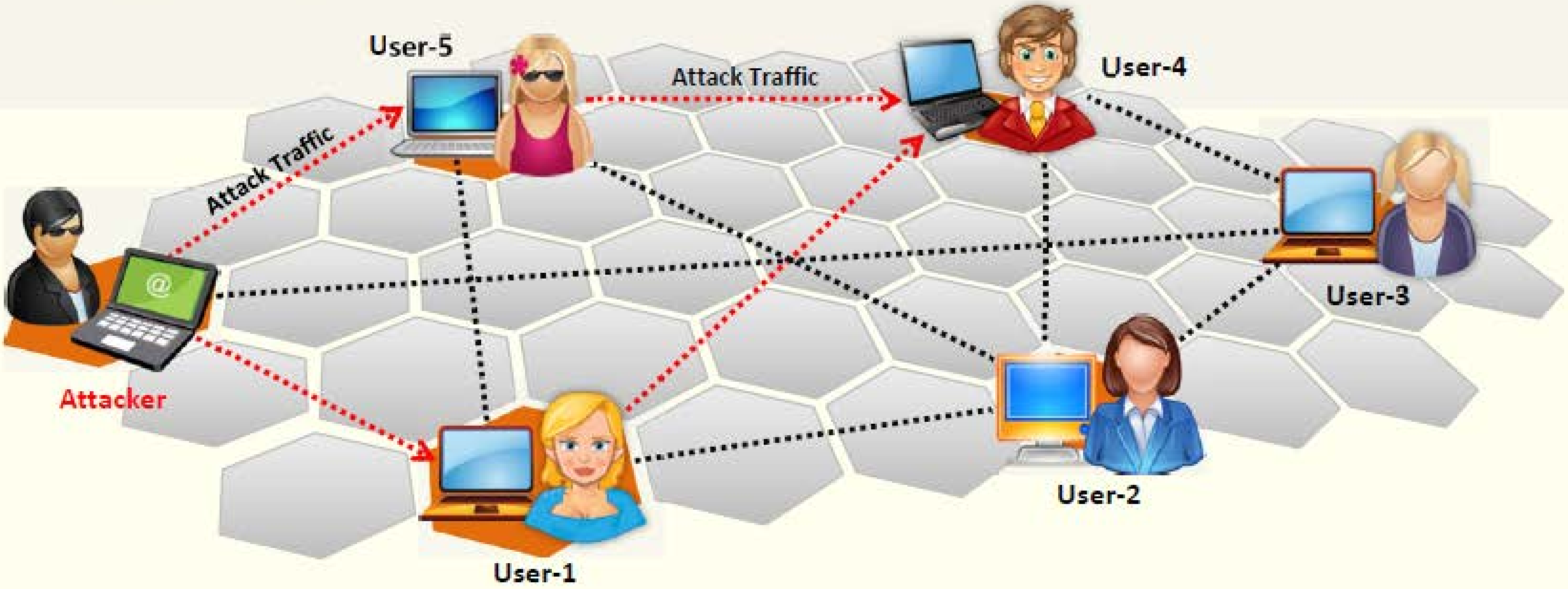
4 The victim's listen queue is **quickly filled up**

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

**Phlashing**

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

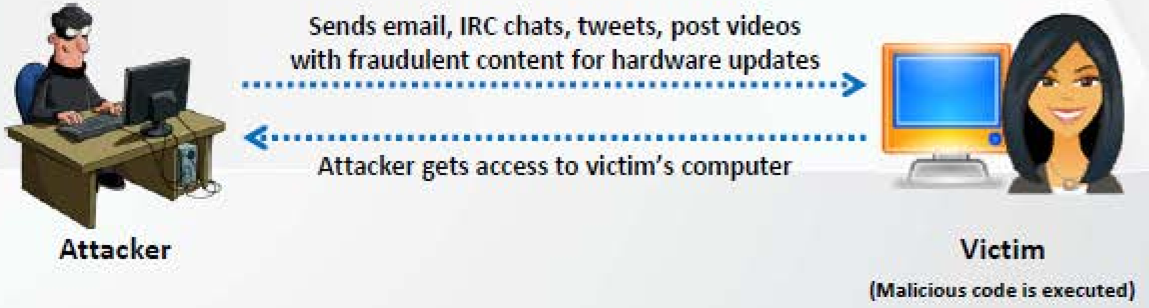
**Sabotage**

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

**Bricking a system**

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

**Process**



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

Attacker gets access to victim's computer

Attacker

Victim

(Malicious code is executed)

# Permanent Denial-of-Service Attack

**Phlashing**

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

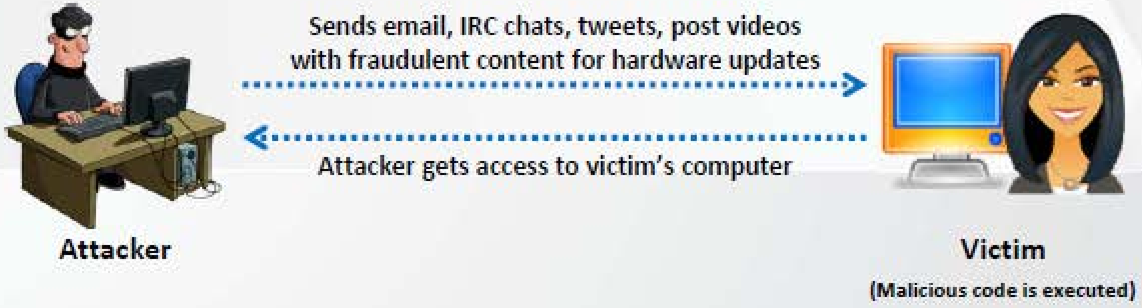
**Sabotage**

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

**Bricking a system**

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

**Process**

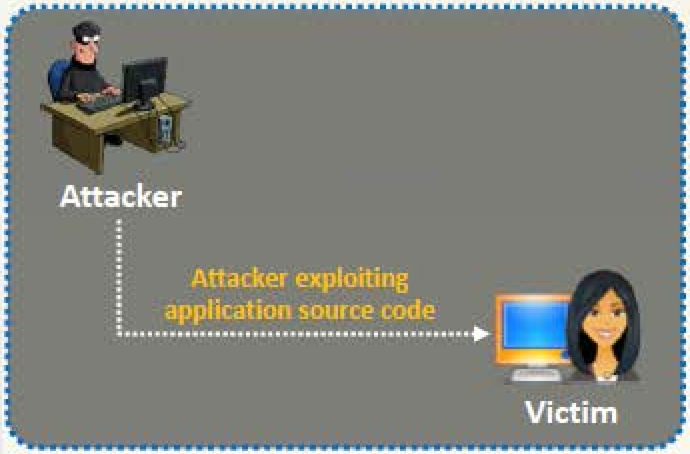

Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates
Attacker gets access to victim's computer
Attacker
Victim
(Malicious code is executed)

# Application-Level Flood Attacks

- 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

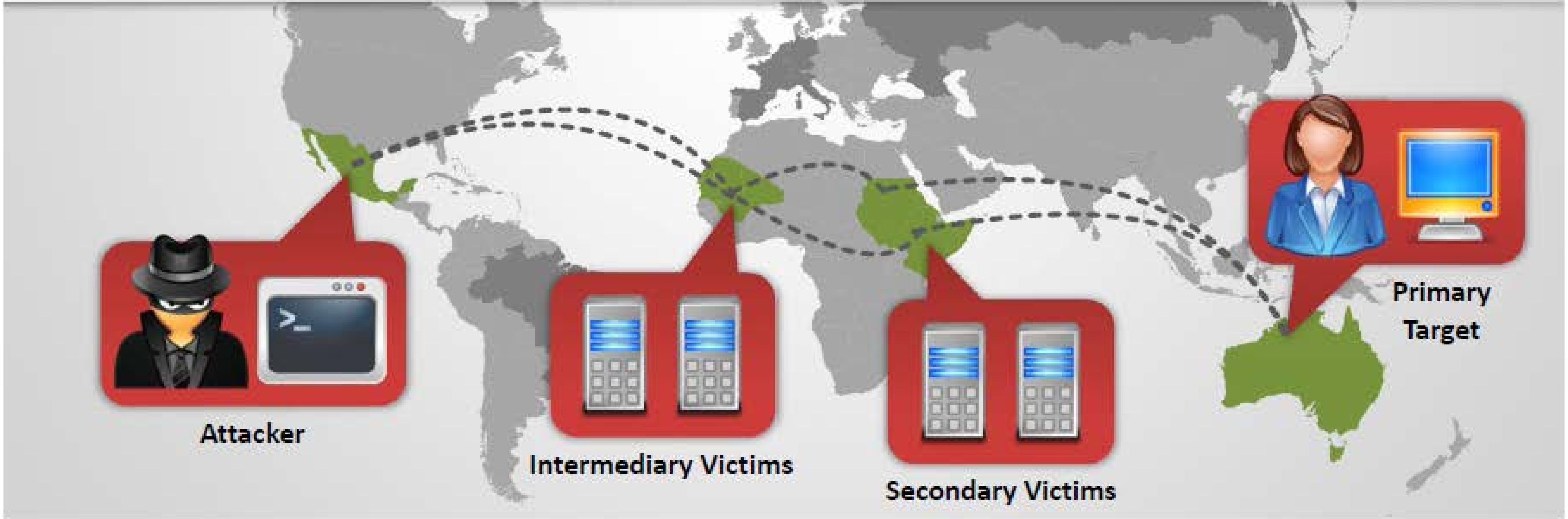
### Using application-level flood attacks, attackers attempts to:

- 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)

- 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**



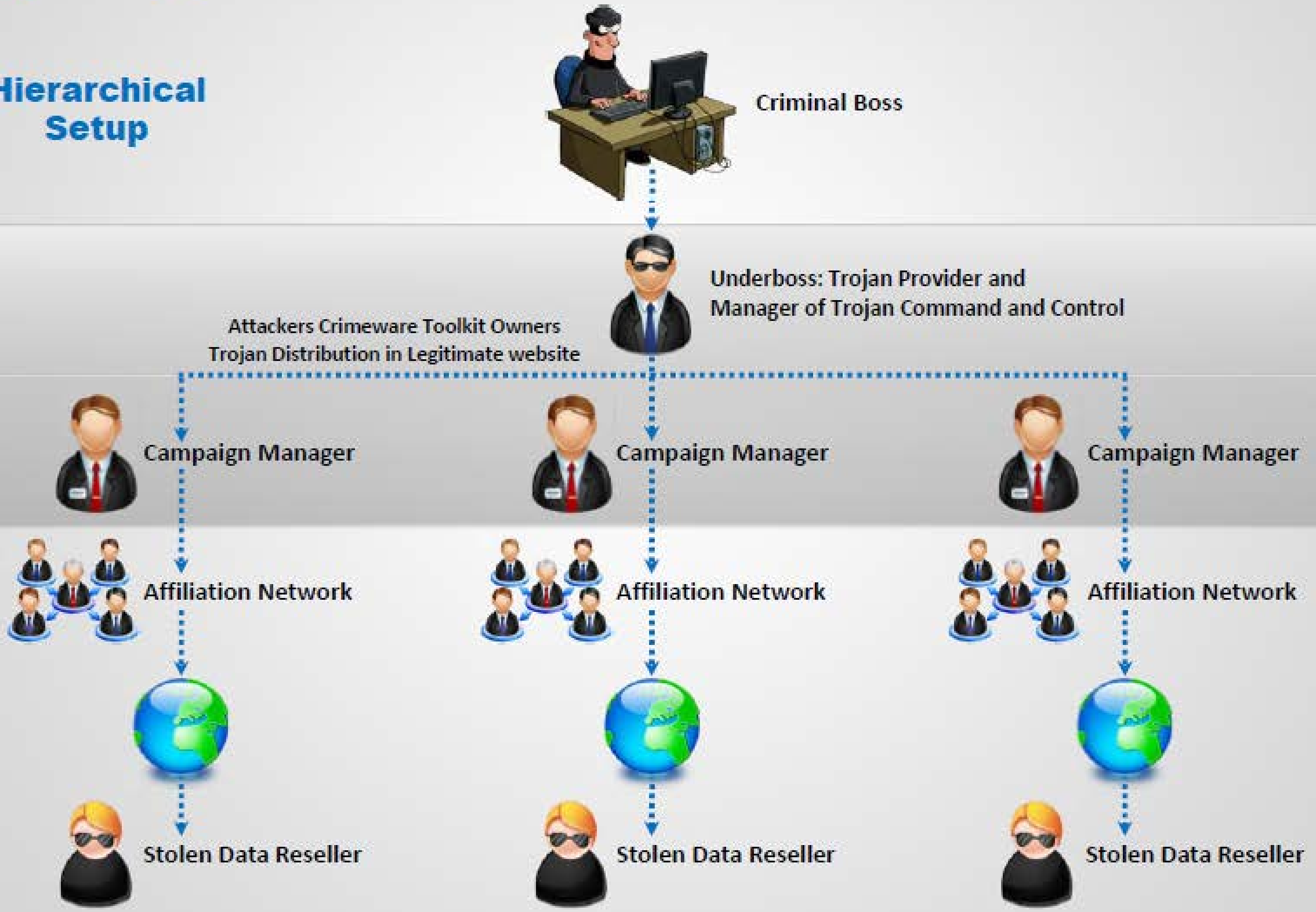
# Module Flow

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

C|EH Certified Ethical Hacker

## Hierarchical Setup



Criminal Boss

Underboss: Trojan Provider and Manager of Trojan Command and Control

Attackers Crimeware Toolkit Owners Trojan Distribution in Legitimate website

Campaign Manager

Campaign Manager

Campaign Manager

Affiliation Network

Affiliation Network

Affiliation Network

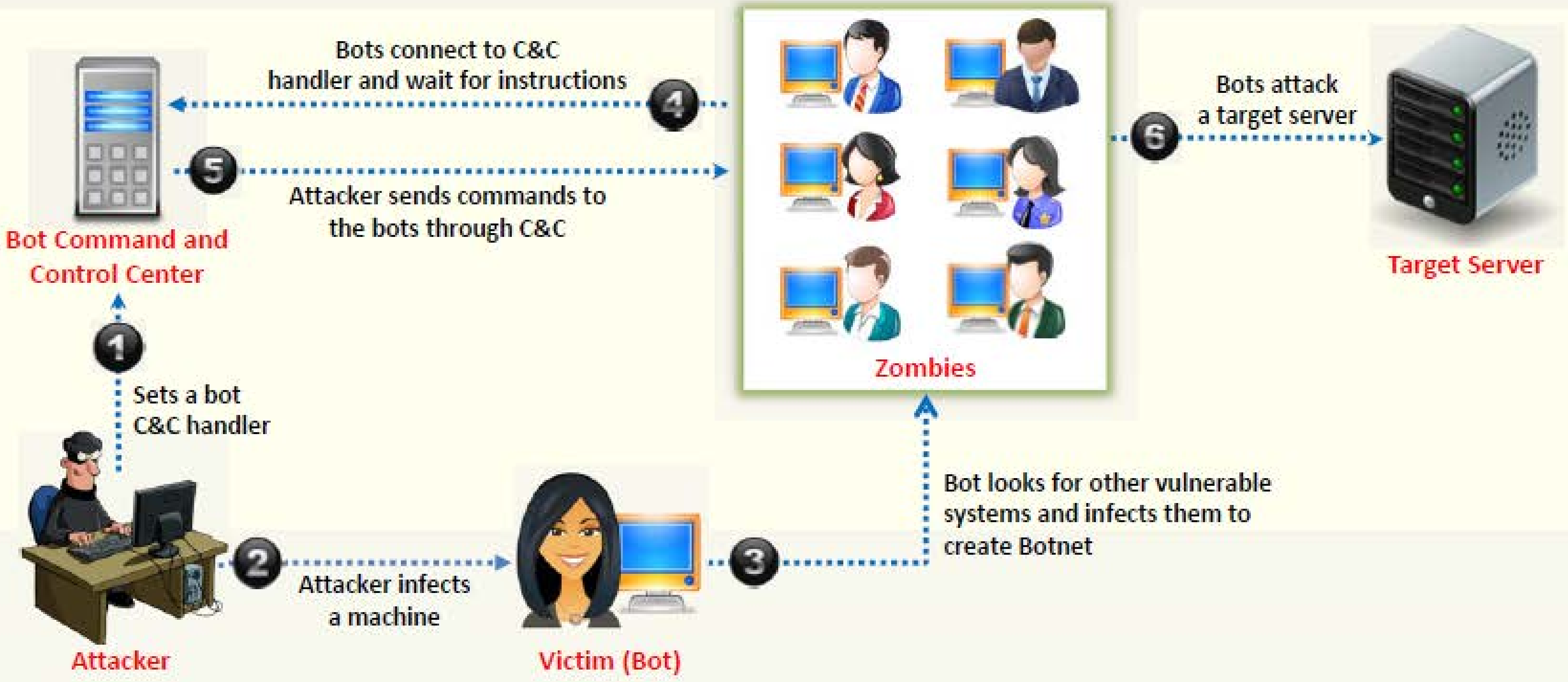
Stolen Data Reseller

Stolen Data Reseller

Stolen Data Reseller

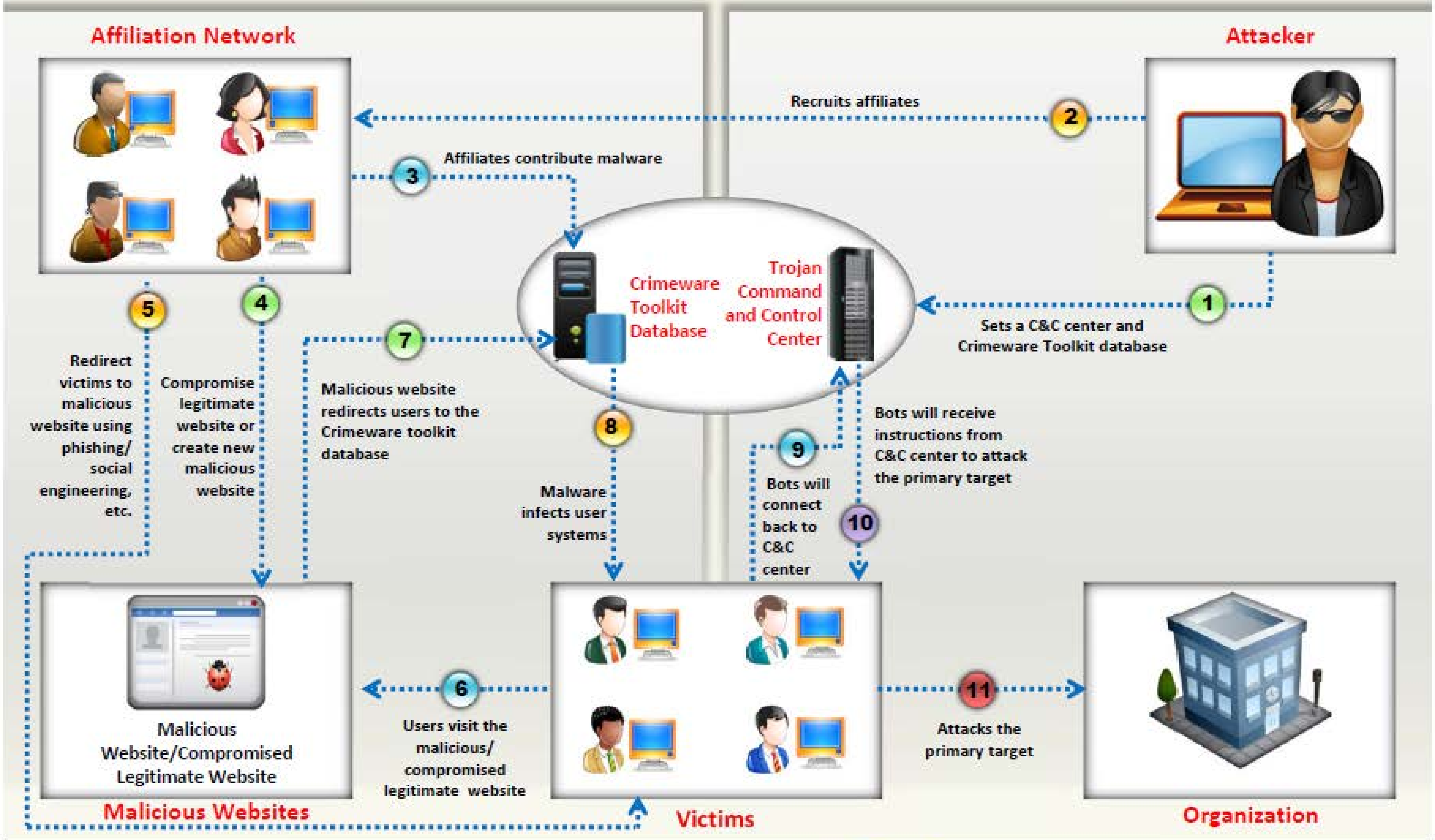
# Botnet

- 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**



Bots connect to C&C handler and wait for instructions
4
5
Attacker sends commands to the bots through C&C
Bot Command and Control Center
Zombies
6
Bots attack a target server
Target Server
1
Sets a bot C&C handler
Attacker
2
Attacker infects a machine
Victim (Bot)
3
Bot looks for other vulnerable systems and infects them to create Botnet

# A Typical Botnet Setup



Affiliation Network

Attacker

Recruits affiliates 2

3 Affiliates contribute malware

Crimeware Toolkit Database

Trojan Command and Control Center

1 Sets a C&C center and Crimeware Toolkit database

5 Redirect victims to malicious website using phishing/ social engineering, etc.

4 Compromise legitimate website or create new malicious website

7 Malicious website redirects users to the Crimeware toolkit database

8 Malware infects user systems

9 Bots will connect back to C&C center

10 Bots will receive instructions from C&C center to attack the primary target

Malicious Website/Compromised Legitimate Website

Malicious Websites

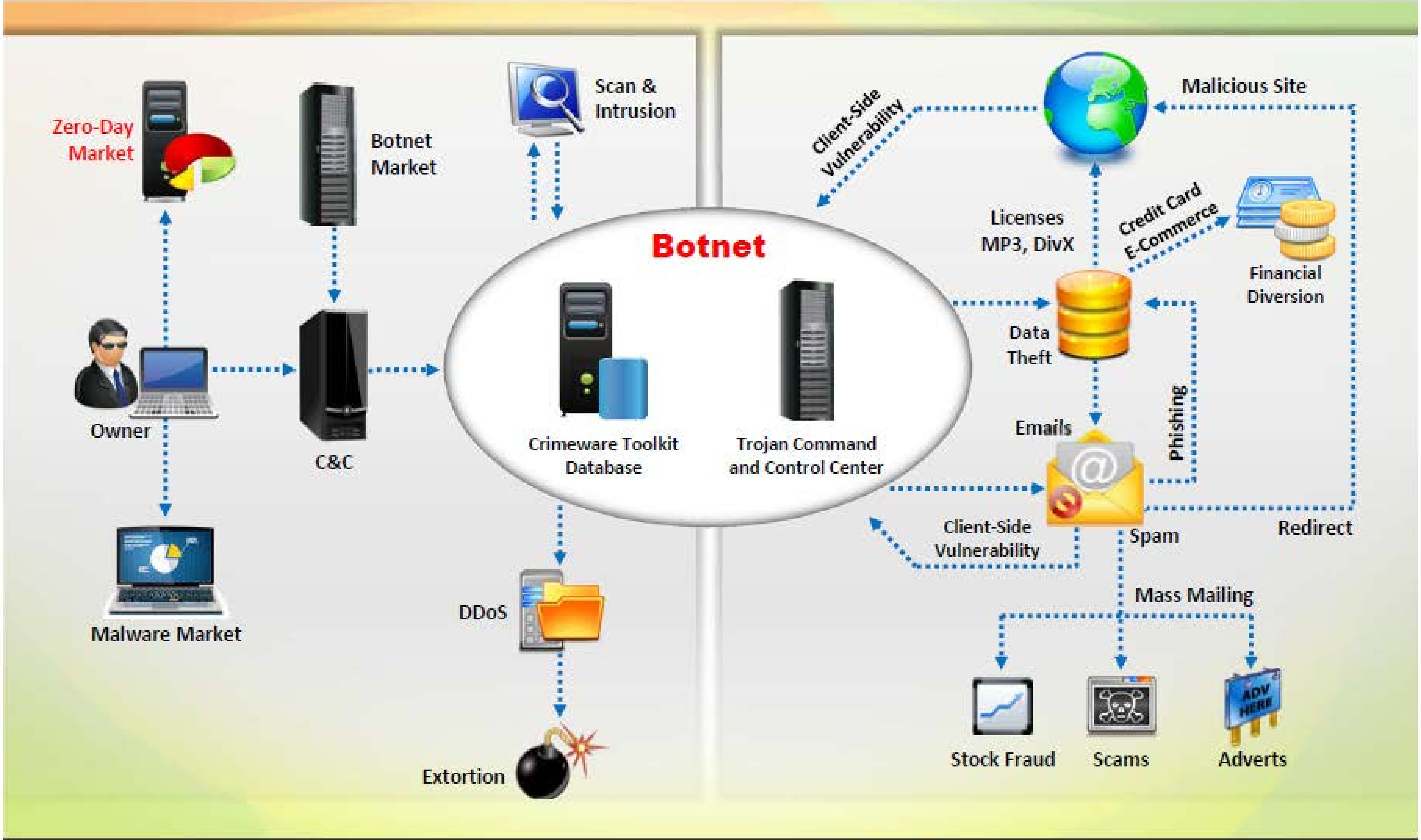
6 Users visit the malicious/ compromised legitimate website

Victims

11 Attacks the primary target

Organization

# Botnet Ecosystem



# 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**

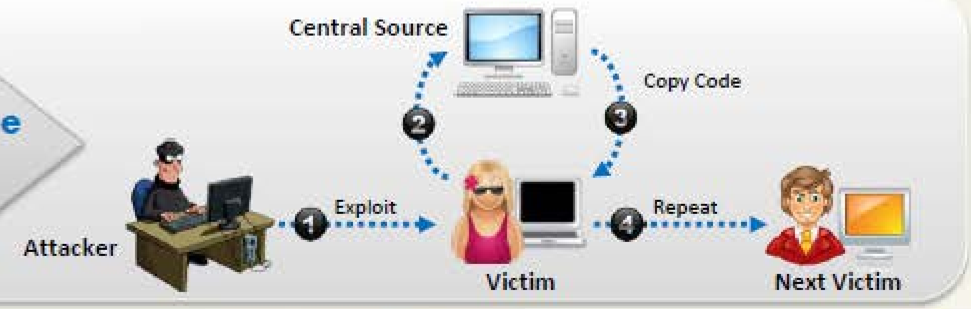
It uses **pseudorandom permutation list of IP addresses** to find new vulnerable machines

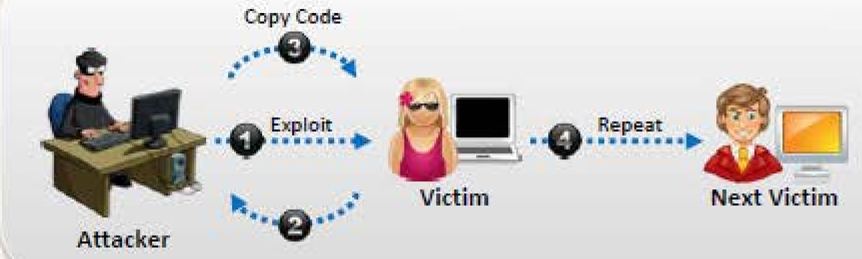
# How Malicious Code Propagates?

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**



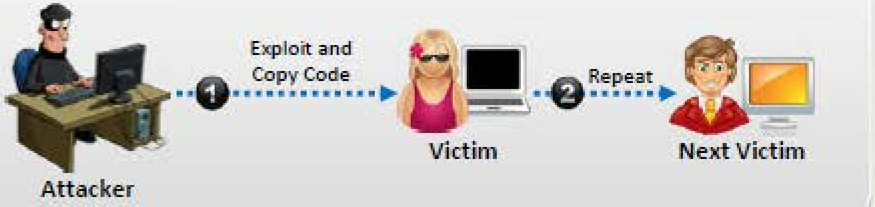


**Back-chaining Propagation**

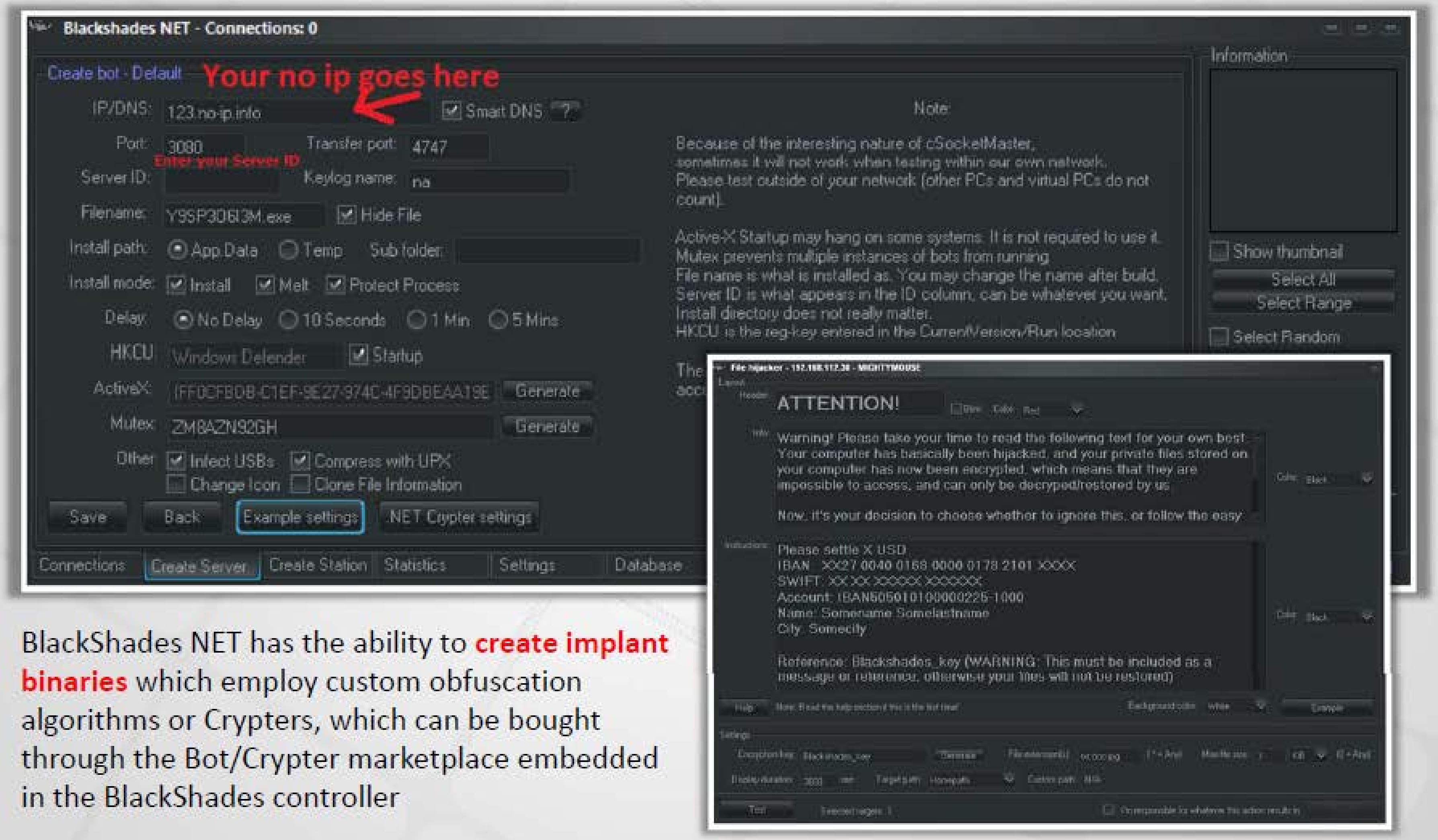
Attacker places **attack toolkit on his/her system itself** and copy of the attack toolkit is transferred to the newly discovered vulnerable system

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

**Autonomous Propagation**



# Botnet Trojan: Blackshades NET



IP/DNS: 123.no-ip.info ☑ Smart DNS ?

Port: 3080 Transfer port: 4747

Server ID: Keylog name: na

Filename: Y9SP30613M.exe ☑ Hide File

Install path: ● App.Data ○ Temp Sub folder:

Install mode: ☑ Install ☑ Melt ☑ Protect Process

Delay: ● No Delay ○ 10 Seconds ○ 1 Min ○ 5 Mins

HKCU: Windows Defender ☑ Startup

ActiveX: {FF0CFBDB-C1EF-9E27-974C-4F9DBEAA19E

Mutex: ZM8AZN92GH

Other: ☑ Infect USBs ☑ Compress with UPX
□ Change Icon □ Clone File Information

Note:

Because of the interesting nature of cSocketMaster,
sometimes it will not work when testing within our own network.
Please test outside of your network (other PCs and virtual PCs do not count).

Active-X Startup may hang on some systems. It is not required to use it.
Mutex prevents multiple instances of bots from running.
File name is what is installed as. You may change the name after build.
Server ID is what appears in the ID column, can be whatever you want.
Install directory does not really matter.
HKCU is the reg-key entered in the CurrentVersion/Run location

□ Show thumbnail

□ Select Random

Header: ATTENTION! Color: Red

Info:

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

Now, it's your decision to choose whether to ignore this, or follow the easy

Color: Black

Instructions:

Please settle X USD
IBAN : XX27 0040 0168 0000 0178 2101 XXXX
SWIFT: XX XX XXXXX XXXXXX
Account: IBAN505010100000225-1000
Name: Somename Somelastname
City: Somecity

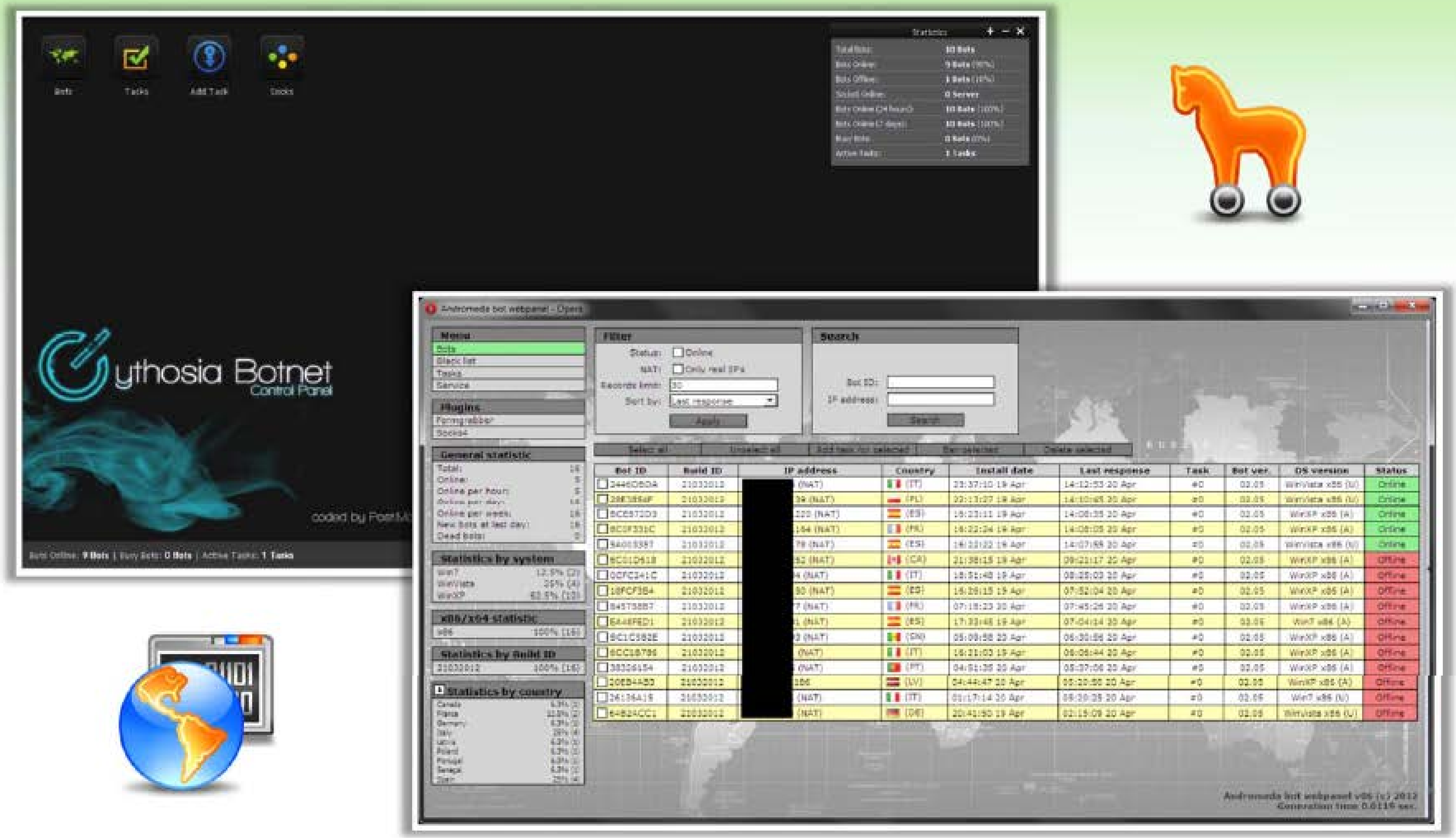
Reference: Blackshades_key (WARNING: This must be included as a message or reference, otherwise your files will not be restored)

Color: Black

Background color: White

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



| | |
|---|---|
| Total Bots: | 10 Bots |
| Bots Online: | 9 Bots (90%) |
| Bots Offline: | 1 Bots (10%) |
| Socks5 Online: | 0 Server |
| Bots Online (24 hours): | 10 Bots (100%) |
| Bots Online (7 days): | 10 Bots (100%) |
| Busy Bots: | 0 Bots (0%) |
| Active Tasks: | 1 Tasks |

Bots Online: 9 Bots | Busy Bots: 0 Bots | Active Tasks: 1 Tasks

Status: □ Online
NAT: □ Only real IPs
Records limit: 30
Sort by: Last response

Bot ID:
IP address:

General statistic

| | |
|---|---|
| Total: | 16 |
| Online: | 5 |
| Online per hour: | 5 |
| Online per day: | 16 |
| Online per week: | 16 |
| New bots at last day: | 16 |
| Dead bots: | 0 |

Statistics by system

| | |
|---|---|
| Win7 | 12.5% (2) |
| WinVista | 25% (4) |
| WinXP | 62.5% (10) |

x86/x64 statistic

| | |
|---|---|
| x86 | 100% (16) |

Statistics by Build ID

| | |
|---|---|
| 21032012 | 100% (16) |

Statistics by country

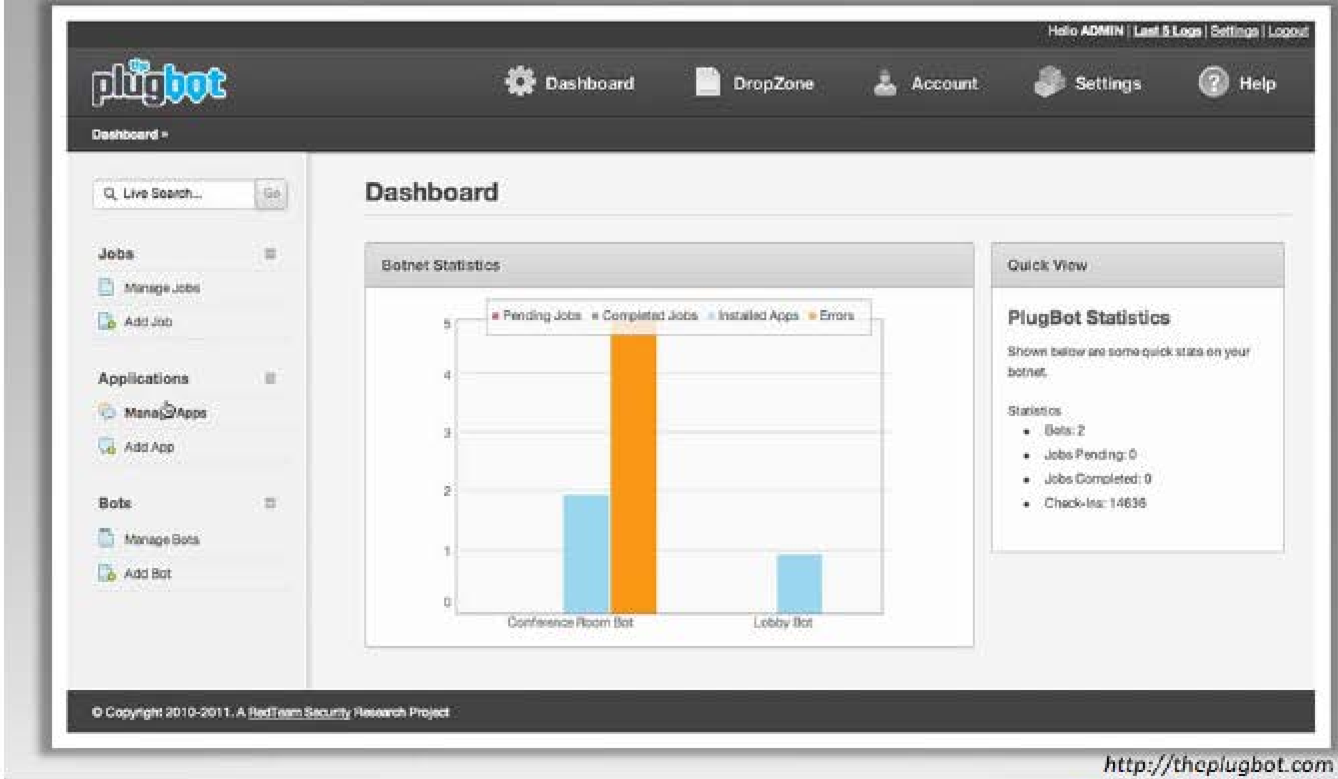
| | |
|---|---|
| Canada | 6.3% (1) |
| France | 12.5% (2) |
| Germany | 6.3% (1) |
| Italy | 25% (4) |
| Latvia | 6.3% (1) |
| Poland | 6.3% (1) |
| Portugal | 6.3% (1) |
| Senegal | 6.3% (1) |
| Spain | 25% (4) |

| Bot ID | Build ID | IP address | Country | Install date | Last response | Task | Bot ver. | OS version | Status |
|---|---|---|---|---|---|---|---|---|---|
| □ 2446D5DA | 21032012 | [redacted] (NAT) | (IT) | 23:37:10 19 Apr | 14:12:53 20 Apr | #0 | 02.05 | WinVista x86 (U) | Online |
| □ 28E3B54F | 21032012 | [redacted] 39 (NAT) | (PL) | 22:13:27 19 Apr | 14:10:05 20 Apr | #0 | 02.05 | WinVista x86 (U) | Online |
| □ 8CE572D3 | 21032012 | [redacted] 220 (NAT) | (ES) | 16:23:11 19 Apr | 14:08:35 20 Apr | #0 | 02.05 | WinXP x86 (A) | Online |
| □ 8C0F331C | 21032012 | [redacted] 184 (NAT) | (FR) | 16:22:24 19 Apr | 14:08:05 20 Apr | #0 | 02.05 | WinXP x86 (A) | Online |
| □ 9A0033B7 | 21032012 | [redacted] 79 (NAT) | (ES) | 16:22:22 19 Apr | 14:07:55 20 Apr | #0 | 02.05 | WinVista x86 (U) | Online |
| □ 8C01D618 | 21032012 | [redacted] 52 (NAT) | (CA) | 21:38:15 19 Apr | 09:21:17 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 0CFC241C | 21032012 | [redacted] 4 (NAT) | (IT) | 18:51:48 19 Apr | 08:25:03 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 18FCF3B4 | 21032012 | [redacted] 30 (NAT) | (ES) | 16:26:15 19 Apr | 07:52:04 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 845758B7 | 21032012 | [redacted] 7 (NAT) | (FR) | 07:18:23 20 Apr | 07:45:26 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 6A4EFED1 | 21032012 | [redacted] 1 (NAT) | (ES) | 17:33:48 19 Apr | 07:04:14 20 Apr | #0 | 02.05 | Win7 x86 (A) | Offline |
| □ 8C1C382E | 21032012 | [redacted] 3 (NAT) | (SN) | 05:09:58 20 Apr | 06:30:56 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 8CC18786 | 21032012 | [redacted] (NAT) | (IT) | 16:21:03 19 Apr | 06:06:44 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 38206154 | 21032012 | [redacted] (NAT) | (PT) | 04:51:35 20 Apr | 05:37:06 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 20EB4A80 | 21032012 | [redacted] 186 | (LV) | 04:44:47 20 Apr | 05:20:56 20 Apr | #0 | 02.05 | WinXP x86 (A) | Offline |
| □ 26136A15 | 21032012 | [redacted] (NAT) | (IT) | 01:17:14 20 Apr | 03:30:35 20 Apr | #0 | 02.05 | Win7 x86 (U) | Offline |
| □ 64B2ACC1 | 21032012 | [redacted] (NAT) | (DE) | 20:41:50 19 Apr | 02:15:09 20 Apr | #0 | 02.05 | WinVista x86 (U) | Offline |

Andromeda bot webpanel v05 (c) 2012
Generation time 0.0116 sec.

# Botnet Trojan: PlugBot

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



Dashboard

PlugBot Statistics

Shown below are some quick stats on your botnet.

Statistics

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

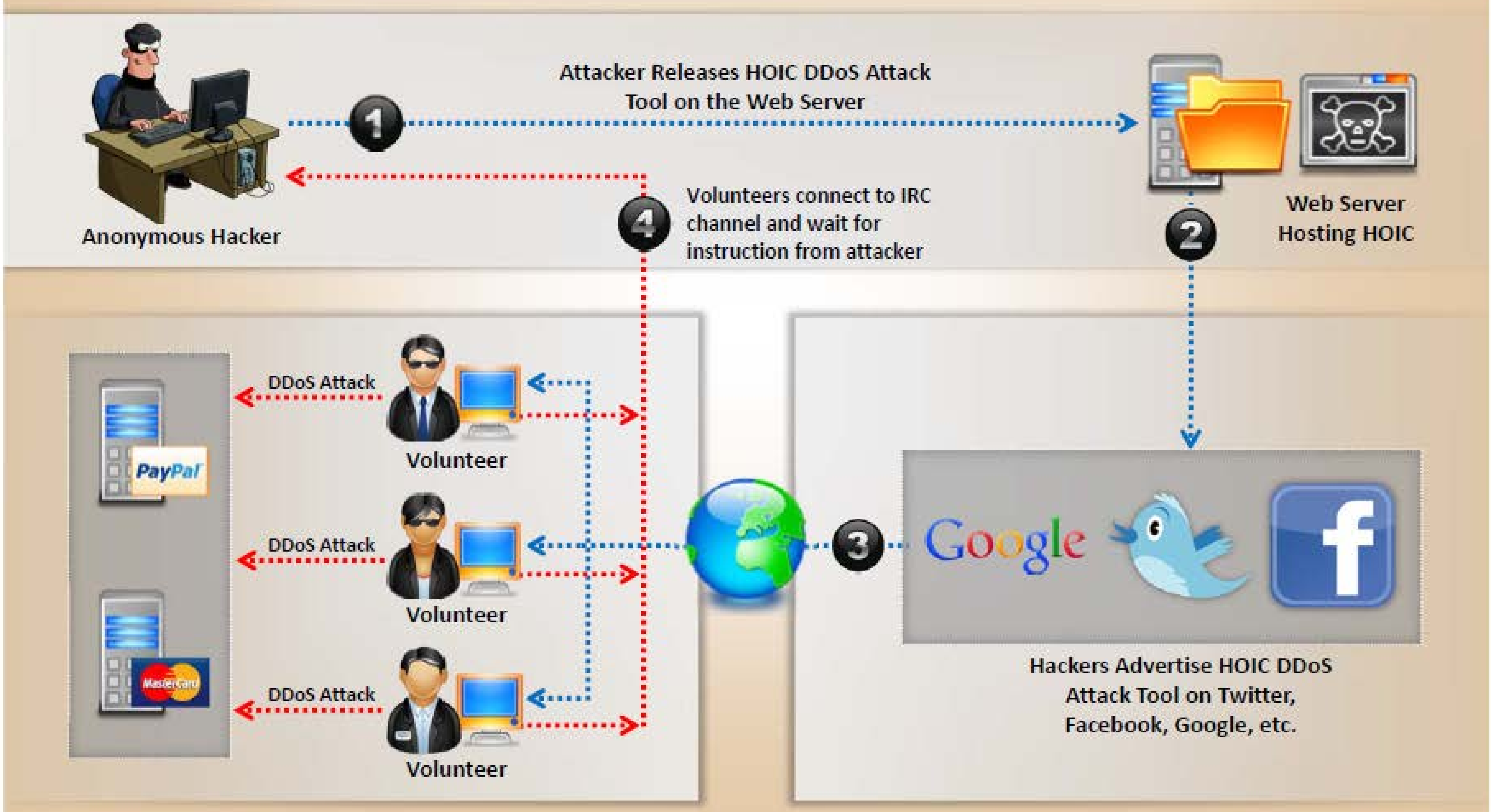
© Copyright 2010-2011. A RedTeam Security Research Project

http://theplugbot.com

# Module Flow

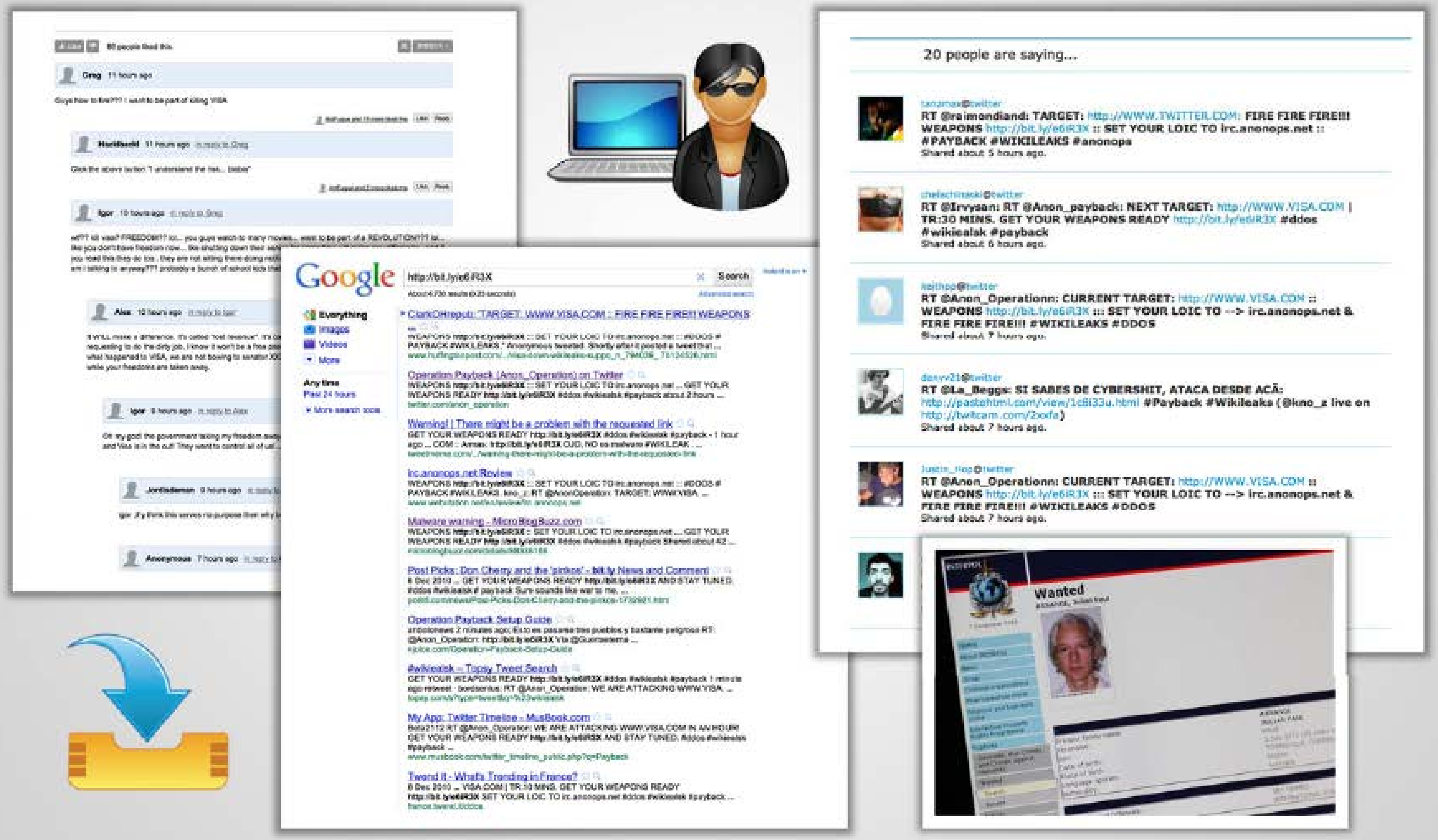
1. DoS/DDoS Concepts
2. DoS/DDoS Attack Techniques
3. Botnets
4. DDoS Case Study
5. DoS/DDoS Attack Tools
6. Countermeasures
7. DoS/DDoS Protection Tools
8. DoS/DDoS Penetration Testing

# DDoS Attack



Anonymous Hacker
1
Attacker Releases HOIC DDoS Attack Tool on the Web Server
Web Server Hosting HOIC
2
4
Volunteers connect to IRC channel and wait for instruction from attacker
DDoS Attack
Volunteer
DDoS Attack
Volunteer
DDoS Attack
Volunteer
PayPal
MasterCard
3
Google
f
Hackers Advertise HOIC DDoS Attack Tool on Twitter, Facebook, Google, etc.

# Hackers Advertise Links to Download Botnet



80 people liked this.

**Greg** 11 hours ago

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

**Hardtbankl** 11 hours ago in reply to Greg

Click the above button "I understand the risk... blabla"

**Igor** 10 hours ago in reply to Greg

wtf?? kill visa? FREEDOM?? lol... you guys watch to many movies... want to be part of a REVOLUTION?? lol... like you don't have freedom now... like shutting down their ... you read this they do too . they are not sitting there doing noth... am i talking to anyway??? probably a bunch of school kids tha...

**Alex** 10 hours ago in reply to Igor

It WILL make a difference. It's called "civil revolution". It's ca... requesting to do the dirty job. I know it won't be a free pla... what happened to VISA, we are not bowing to senator XX... while your freedoms are taken away.

**Igor** 9 hours ago in reply to Alex

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

**Jontisdaman** 8 hours ago in reply to...

Igor ,If y think this serves no purpose then why ...

**Anonymous** 7 hours ago in reply to...

http://bit.ly/e6iR3X

About 4,730 results (0.23 seconds)

Everything
Images
Videos
More

Any time
Past 24 hours
More search tools

**ClarkOHreport: "TARGET: WWW.VISA.COM :: FIRE FIRE FIRE!!! WEAPONS ...**
WEAPONS http://bit.ly/e6iR3X :: SET YOUR LOIC TO irc.anonops.net :: #DDOS # PAYBACK #WIKILEAKS," Anonymous tweeted. Shortly after it posted a tweet that ...
www.huffingtonpost.com/.../visa-down-wikileaks-suppo_n_794036_75124526.html

**Operation Payback (Anon_Operation) on Twitter**
WEAPONS http://bit.ly/e6iR3X :: SET YOUR LOIC TO irc.anonops.net ... GET YOUR WEAPONS READY http://bit.ly/e6iR3X #ddos #wikileaks #payback about 2 hours ...
twitter.com/anon_operation

**Warning! | There might be a problem with the requested link**
GET YOUR WEAPONS READY http://bit.ly/e6iR3X #ddos #wikileaks #payback - 1 hour ago ... COM :: Armas: http://bit.ly/e6iR3X OJO, NO es malware #WIKILEAK ...
tweetmeme.com/.../warning-there-might-be-a-problem-with-the-requested-link

**irc.anonops.net Review**
WEAPONS http://bit.ly/e6iR3X :: SET YOUR LOIC TO irc.anonops.net :: #DDOS # PAYBACK #WIKILEAKS. kno_z: RT @AnonOperation: TARGET: WWW.VISA ...
www.websitelooker.net/en/review/irc.anonops.net

**Malware warning - MicroBlogBuzz.com**
WEAPONS http://bit.ly/e6iR3X :: SET YOUR LOIC TO irc.anonops.net ... GET YOUR WEAPONS READY http://bit.ly/e6iR3X #ddos #wikileaks #payback Shared about 42 ...
microblogbuzz.com/details/98506188

**Post Picks: Don Cherry and the 'pinkos' - bit.ly News and Comment**
8 Dec 2010 ... GET YOUR WEAPONS READY http://bit.ly/e6iR3X AND STAY TUNED. #ddos #wikileaks # payback Sure sounds like war to me. ...
posted.com/news/Post-Picks-Don-Cherry-and-the-pinkos-1732921.html

**Operation Payback Setup Guide**
anpolonews 2 minutes ago; Esto es pasarse tres pueblos y bastante peligroso RT: @Anon_Operation: http://bit.ly/e6iR3X Via @Guerraeterna ...
ejulce.com/Operation-Payback-Setup-Guide

**#wikileaks - Topsy Tweet Search**
GET YOUR WEAPONS READY http://bit.ly/e6iR3X #ddos #wikileaks #payback 1 minute ago retweet · bordsonius: RT @Anon_Operation: WE ARE ATTACKING WWW.VISA. ...
topsy.com/s?type=tweet&q=%23wikileaks

**My App: Twitter Timeline - MusBook.com**
Beta2112 RT @Anon_Operation: WE ARE ATTACKING WWW.VISA.COM IN AN HOUR! GET YOUR WEAPONS READY http://bit.ly/e6iR3X AND STAY TUNED. #ddos #wikileaks #payback ...
www.musbook.com/twitter_timeline_public.php?q=Payback

**Twend it - Whats Trending in France?**
8 Dec 2010 ... VISA.COM | TR:10 MINS. GET YOUR WEAPONS READY http://bit.ly/e6iR3X SET YOUR LOIC TO irc.anonops.net #ddos #wikileaks #payback ...
france.twend.it/ddos

20 people are saying...

tanamax@twitter
**RT @raimondiand: 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.

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

keithpo@twitter
**RT @Anon_Operationn: 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.

danyv21@twitter
**RT @La_Beggs: SI SABES DE CYBERSHIT, ATACA DESDE ACÃ: http://pastehtml.com/view/1c8i33u.html #Payback #Wikileaks (@kno_z live on http://twitcam.com/2xxfa)**
Shared about 7 hours ago.

Justin_Hop@twitter
**RT @Anon_Operationn: 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.

# 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

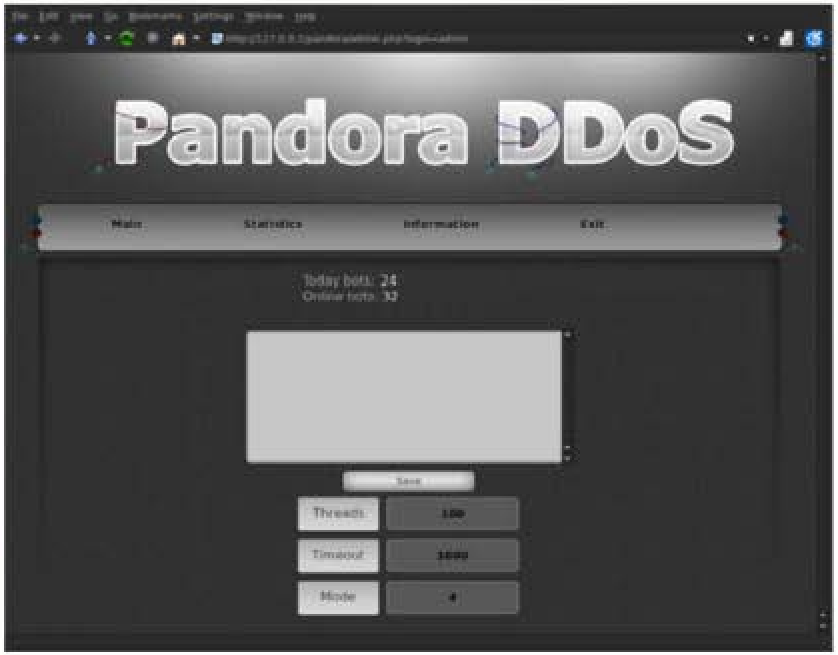
C|EH Certified Ethical Hacker

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



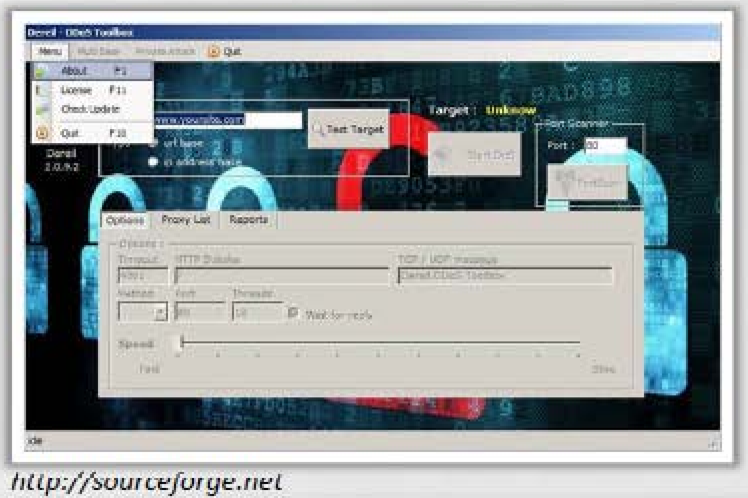
Today bots: 24
Online bots: 32

Threads: 100

Timeout: 1000

Mode: 4

# DoS and DDoS Attack Tools: Dereil and HOIC



www.yoursite.com

url base

ip address base

Target : Unknow

Port : 80

Timeout: 9001

TCP / UDP message: Dereil DDoS Toolbox

Port: 80

Threads: 10

Wait for reply

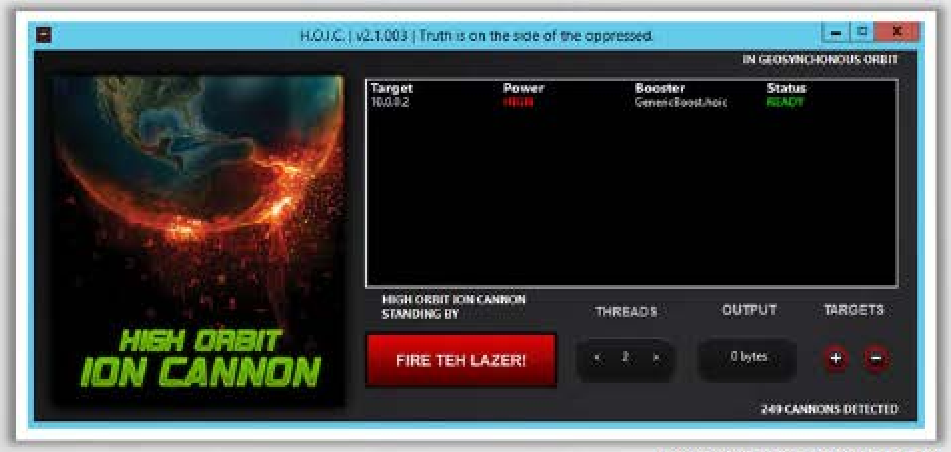
http://sourceforge.net

## 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



| Target | Power | Booster | Status |
|---|---|---|---|
| 10.0.0.2 | HIGH | GenericBoost.hoic | READY |

THREADS: 2

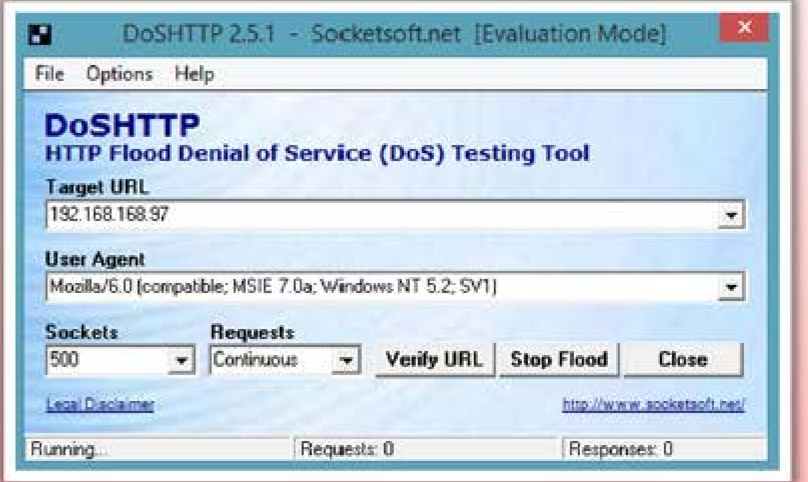
OUTPUT: 0 bytes

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


DoSHTTP 2.5.1 - Socketsoft.net [Evaluation Mode]
File
Options
Help
Verify URL
Stop Flood
Close
Legal Disclaimer
http://www.socketsoft.net/

DoSHTTP
HTTP Flood Denial of Service (DoS) Testing Tool

Target URL: 192.168.168.97

User Agent: Mozilla/6.0 (compatible; MSIE 7.0a; Windows NT 5.2; SV1)

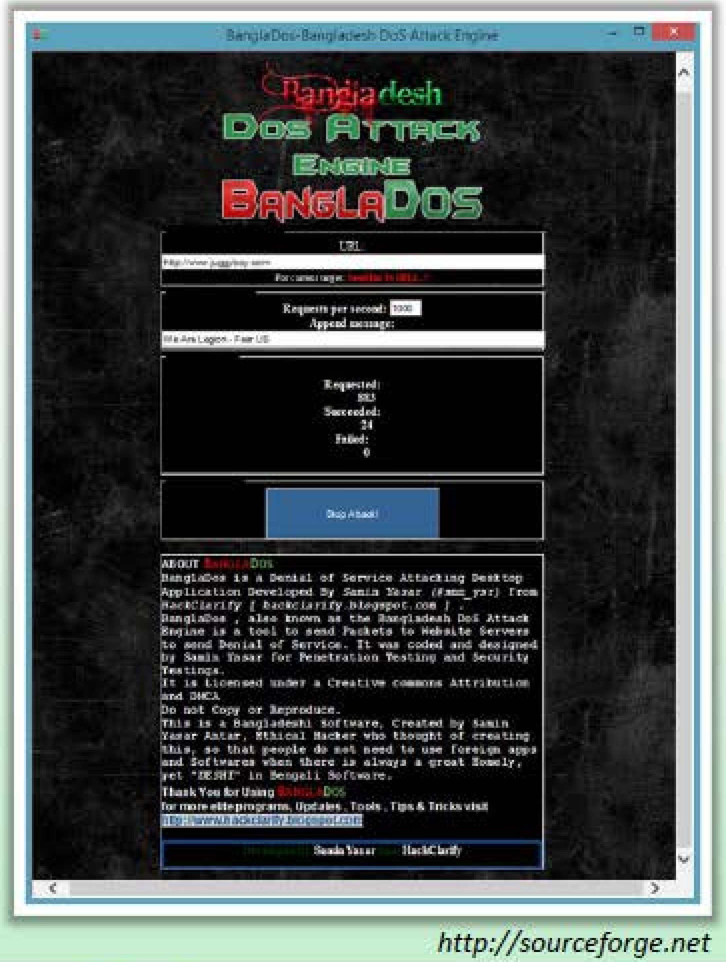
Sockets: 500

Requests: Continuous

Running... | Requests: 0 | Responses: 0

*http://socketsoft.net*

## BanglaDos



URL: http://www.juggyboy.com

For current target: [illegible]

Requests per second: 1000

Append message: We Are Legion - Fear US

Requested: 883

Succeeded: 24

Failed: 0

ABOUT BanglaDos

BanglaDos is a Denial of Service Attacking Desktop Application Developed By Samin Yasar (#smn_ysr) from HackClarify [ hackclarify.blogspot.com ] .
BanglaDos , also known as the Bangladesh DoS Attack Engine is a tool to send Packets to Website Servers to send Denial of Service. It was coded and designed by Samin Yasar for Penetration Testing and Security Testings.
It is Licensed under a Creative commons Attribution and DMCA
Do not Copy or Reproduce.
This is a Bangladeshi Software, Created by Samin Yasar Antar, Ethical Hacker who thought of creating this, so that people do not need to use foreign apps and Softwares when there is always a great Homely, yet "DESHI" in Bengali Software.

Thank You for Using BanglaDos

for more elite programs, Updates , Tools , Tips & Tricks visit http://www.hackclarify.blogspot.com

Samin Yasar HackClarify

*http://sourceforge.net*

# DoS and DDoS Attack Tools

**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*

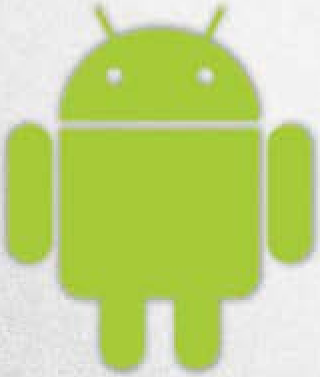
**HULK**
*http://www.sectorix.com*

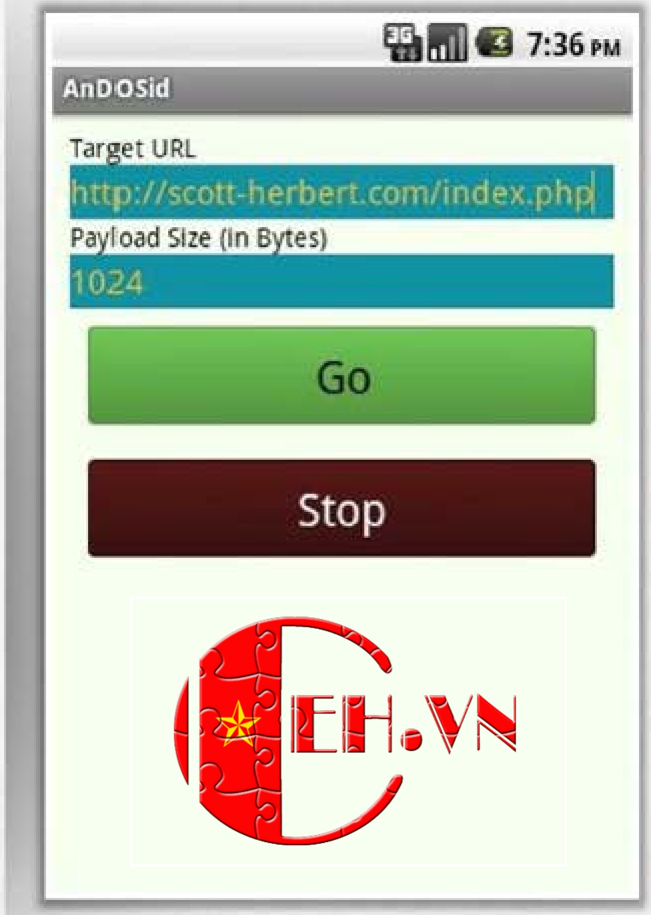
**R-U-Dead-Yet**
*https://code.google.com*

**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





7:36 PM

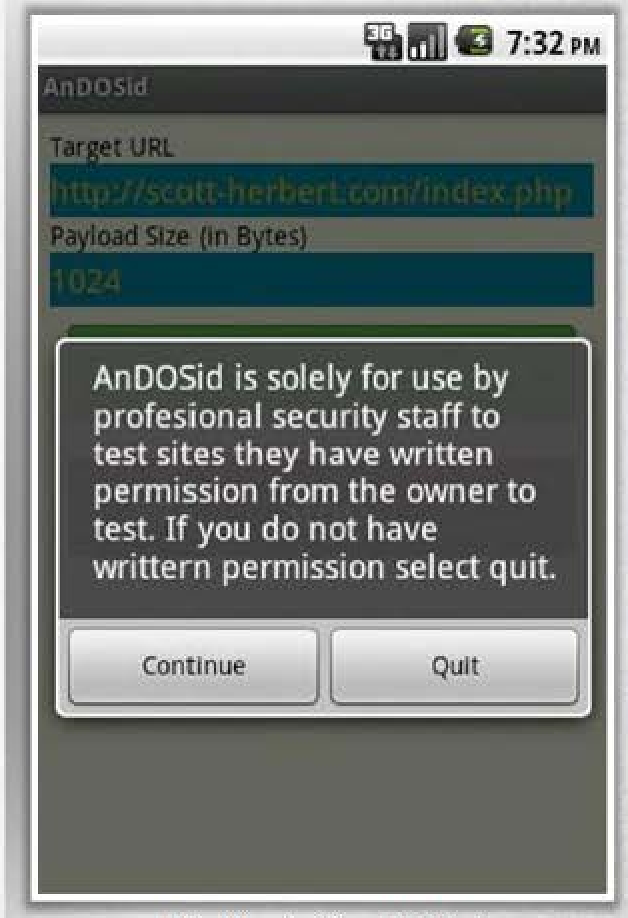
AnDOSid

Target URL

http://scott-herbert.com/index.php

Payload Size (in Bytes)

1024



7:32 PM

AnDOSid

Target URL

http://scott-herbert.com/index.php

Payload Size (in Bytes)

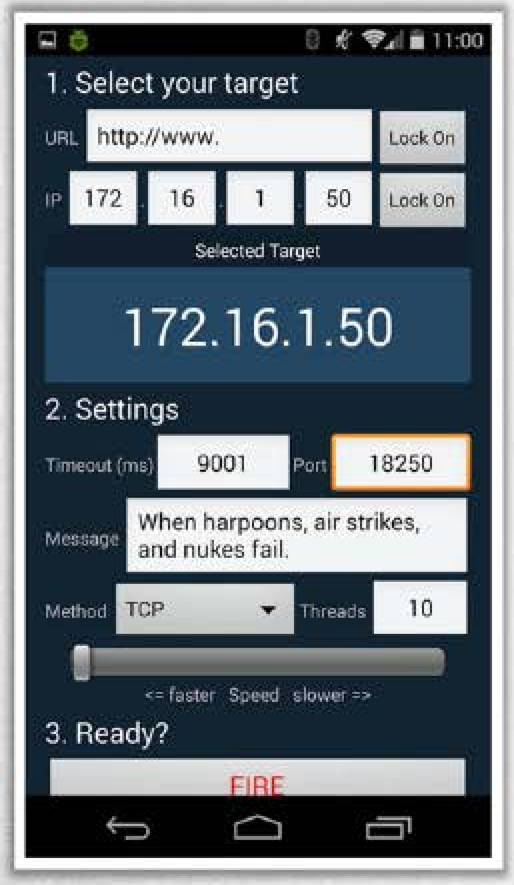
1024

AnDOSid is solely for use by profesional security staff to test sites they have written permission from the owner to test. If you do not have writtern permission select quit.

*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



1. Select your target

URL: http://www. | Lock On

IP: 172 . 16 . 1 . 50 | Lock On

Selected Target

172.16.1.50

2. Settings

Timeout (ms): 9001 | Port: 18250

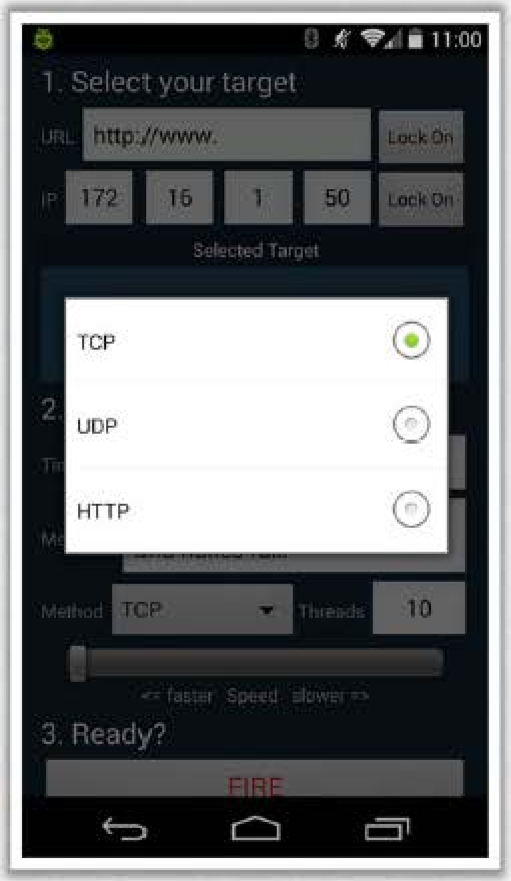
Message: When harpoons, air strikes, and nukes fail.

Method: TCP | Threads: 10

<= faster Speed slower =>

3. Ready?

FIRE



1. Select your target

URL: http://www. | Lock On

IP: 172 . 16 . 1 . 50 | Lock On

Selected Target

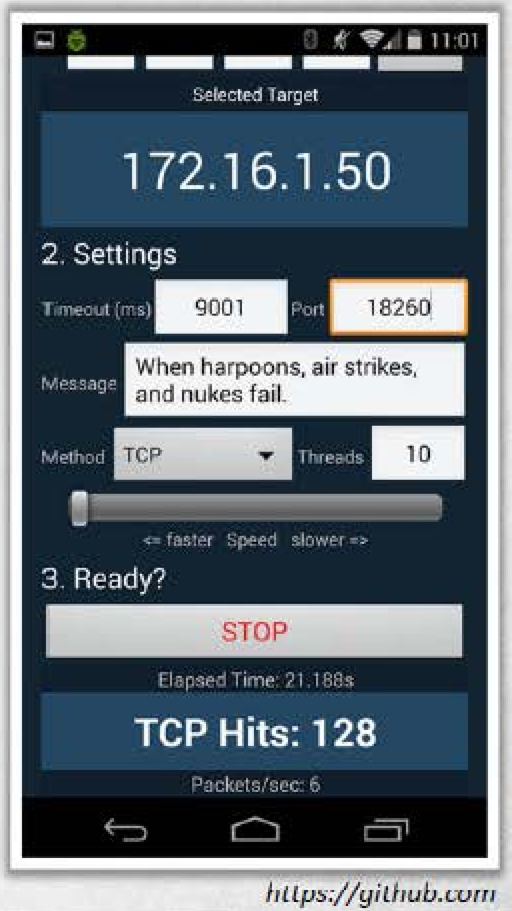
○ TCP ●
UDP ○
HTTP ○

Method: TCP | Threads: 10

<= faster Speed slower =>

3. Ready?

FIRE



Selected Target

172.16.1.50

2. Settings

Timeout (ms): 9001 | Port: 18260

Message: When harpoons, air strikes, and nukes fail.

Method: TCP | Threads: 10

<= faster Speed slower =>

3. Ready?

STOP

Elapsed Time: 21.188s

TCP Hits: 128

Packets/sec: 6

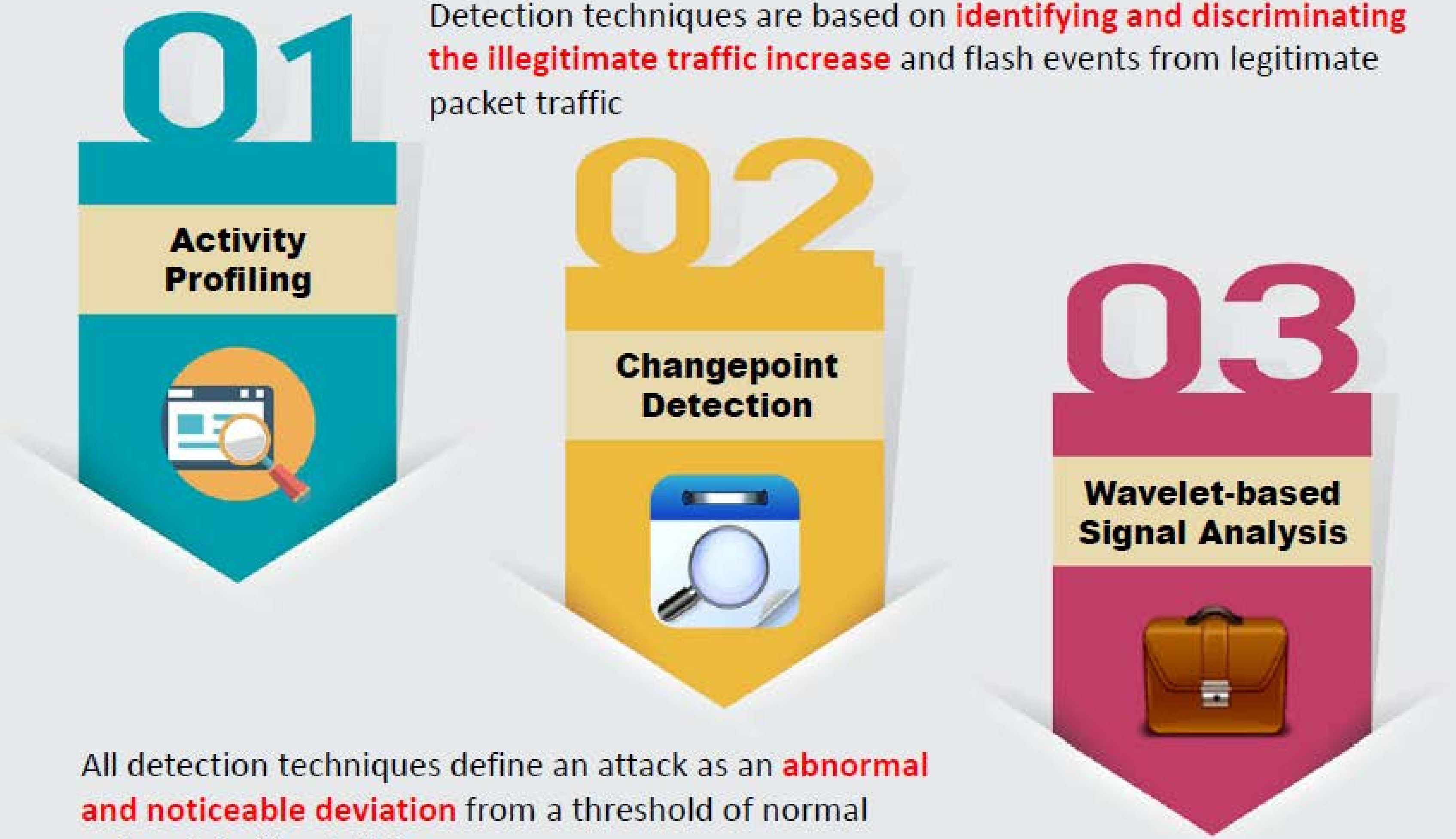
https://github.com

# 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**

Detection techniques are based on **identifying and discriminating the illegitimate traffic increase** and flash events from legitimate packet traffic



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

01

## Absorbing the Attack

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

02

## Degrading Services

- **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

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

## Egress Filtering

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

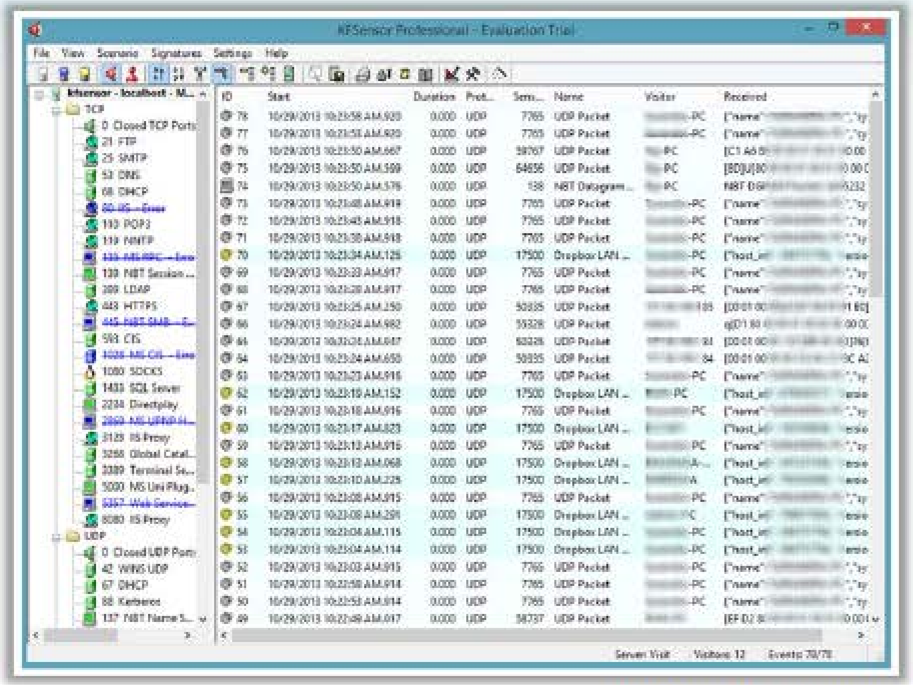
## Ingress Filtering

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

## TCP Intercept

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

# DoS/DDoS Countermeasures: Deflect Attacks



KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help

- kfsensor - localhost - M...
  - TCP
    - 0 Closed TCP Ports
    - 21 FTP
    - 25 SMTP
    - 53 DNS
    - 68 DHCP
    - ~~80 IIS - Error~~
    - 110 POP3
    - 119 NNTP
    - ~~135 MS RPC - Err...~~
    - 139 NBT Session ...
    - 389 LDAP
    - 443 HTTPS
    - ~~445 NBT SMB - E...~~
    - 593 CIS
    - ~~1025 MS CIS - Erro...~~
    - 1080 SOCKS
    - 1433 SQL Server
    - 2234 Directplay
    - ~~2869 MS UPNP N...~~
    - 3128 IIS Proxy
    - 3268 Global Catal...
    - 3389 Terminal Se...
    - 5000 MS Uni Plug...
    - ~~5357 Web Service...~~
    - 8080 IIS Proxy
  - UDP
    - 0 Closed UDP Ports
    - 42 WINS UDP
    - 67 DHCP
    - 88 Kerberos
    - 137 NBT Name S...

| ID | Start | Duration | Prot... | Sens... | Name | Visitor | Received |
|---|---|---|---|---|---|---|---|
| 78 | 10/29/2013 10:23:58 AM.920 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 77 | 10/29/2013 10:23:53 AM.920 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 76 | 10/29/2013 10:23:50 AM.667 | 0.000 | UDP | 59767 | UDP Packet | [redacted]PC | [C1 A6 [redacted] 00 00 |
| 75 | 10/29/2013 10:23:50 AM.599 | 0.000 | UDP | 64656 | UDP Packet | [redacted]PC | [BD]U]80 [redacted] 00 0( |
| 74 | 10/29/2013 10:23:50 AM.576 | 0.000 | UDP | 138 | NBT Datagram ... | [redacted]PC | NBT DG[redacted]0232 |
| 73 | 10/29/2013 10:23:48 AM.919 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 72 | 10/29/2013 10:23:43 AM.918 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 71 | 10/29/2013 10:23:38 AM.918 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 70 | 10/29/2013 10:23:34 AM.125 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]-PC | ["host_in[redacted]"versio |
| 69 | 10/29/2013 10:23:33 AM.917 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 68 | 10/29/2013 10:23:28 AM.917 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 67 | 10/29/2013 10:23:25 AM.250 | 0.000 | UDP | 50535 | UDP Packet | [redacted]105 | [00:01 00[redacted]1 EC] |
| 66 | 10/29/2013 10:23:24 AM.982 | 0.000 | UDP | 55328 | UDP Packet | [redacted] | g[D1 80 [redacted] 00 0( |
| 65 | 10/29/2013 10:23:24 AM.887 | 0.000 | UDP | 60228 | UDP Packet | [redacted]23 | [00:01 00[redacted]]Nj |
| 64 | 10/29/2013 10:23:24 AM.650 | 0.000 | UDP | 50535 | UDP Packet | [redacted]84 | [00:01 00[redacted]C A |
| 63 | 10/29/2013 10:23:23 AM.916 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 62 | 10/29/2013 10:23:19 AM.152 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]-PC | ["host_in[redacted]"versio |
| 61 | 10/29/2013 10:23:18 AM.916 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 60 | 10/29/2013 10:23:17 AM.823 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted] | ["host_in[redacted]"versio |
| 59 | 10/29/2013 10:23:13 AM.916 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 58 | 10/29/2013 10:23:13 AM.068 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]A-... | ["host_in[redacted]"versio |
| 57 | 10/29/2013 10:23:10 AM.225 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]A | ["host_in[redacted]"versio |
| 56 | 10/29/2013 10:23:08 AM.915 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 55 | 10/29/2013 10:23:08 AM.291 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]C | ["host_in[redacted]"versio |
| 54 | 10/29/2013 10:23:04 AM.115 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]-PC | ["host_in[redacted]"versio |
| 53 | 10/29/2013 10:23:04 AM.114 | 0.000 | UDP | 17500 | Dropbox LAN ... | [redacted]-PC | ["host_in[redacted]"versio |
| 52 | 10/29/2013 10:23:03 AM.915 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 51 | 10/29/2013 10:22:58 AM.914 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 50 | 10/29/2013 10:22:53 AM.914 | 0.000 | UDP | 7765 | UDP Packet | [redacted]-PC | ["name"[redacted]","ty |
| 49 | 10/29/2013 10:22:49 AM.017 | 0.000 | UDP | 58737 | UDP Packet | [redacted] | [EF D2 8[redacted]0 001 |

Server: Visit    Visitors: 12    Events: 78/78

*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 IPSes 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

## Throttling

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

# Post-Attack Forensics

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

C|EH Certified Ethical Hacker

## 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

C|EH Certified Ethical Hacker

- 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**
- Perform the thorough **input validation**
- Prevent use of **unnecessary functions** such as gets, strcpy etc.
- Secure the **remote administration** and **connectivity testing**
- Data processed by the attacker should be **stopped from being executed**
- Prevent the **return addresses** from being overwritten

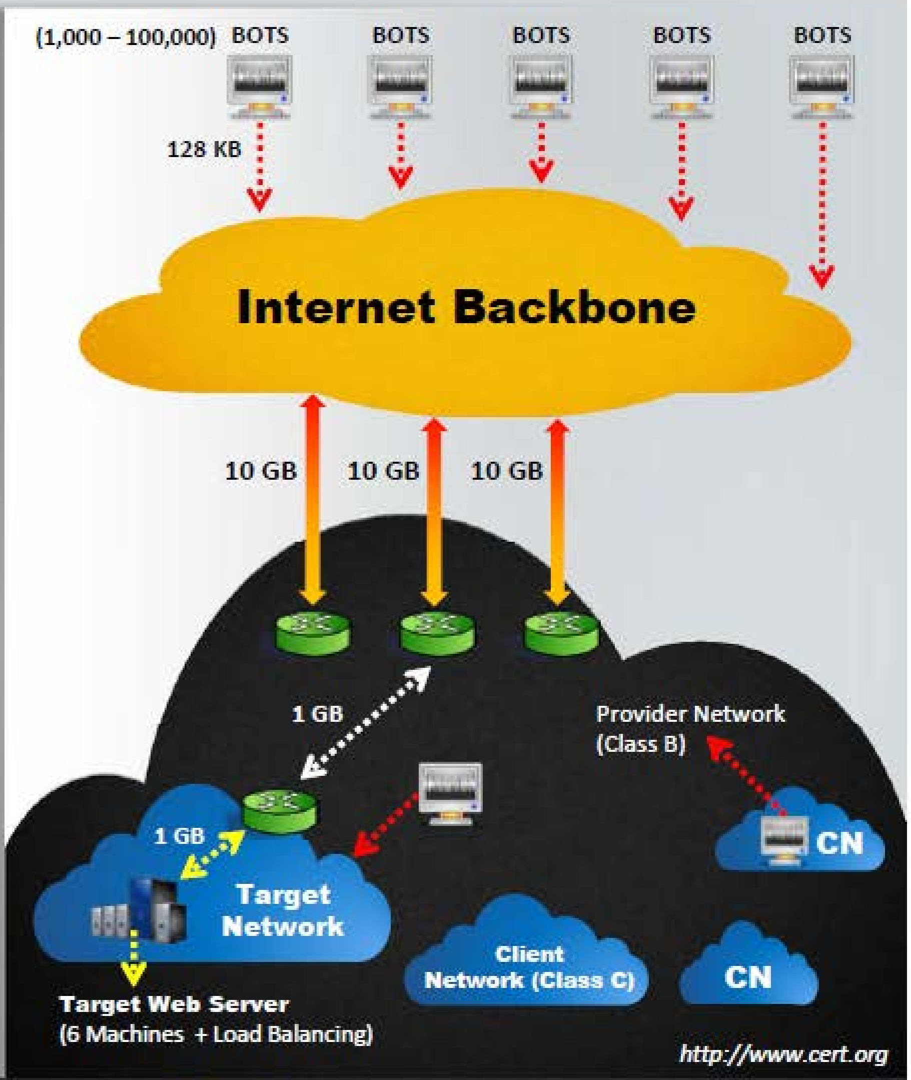
# DoS/DDoS Protection at ISP Level

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



http://www.cert.org

# 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` *access-list-number* | 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**

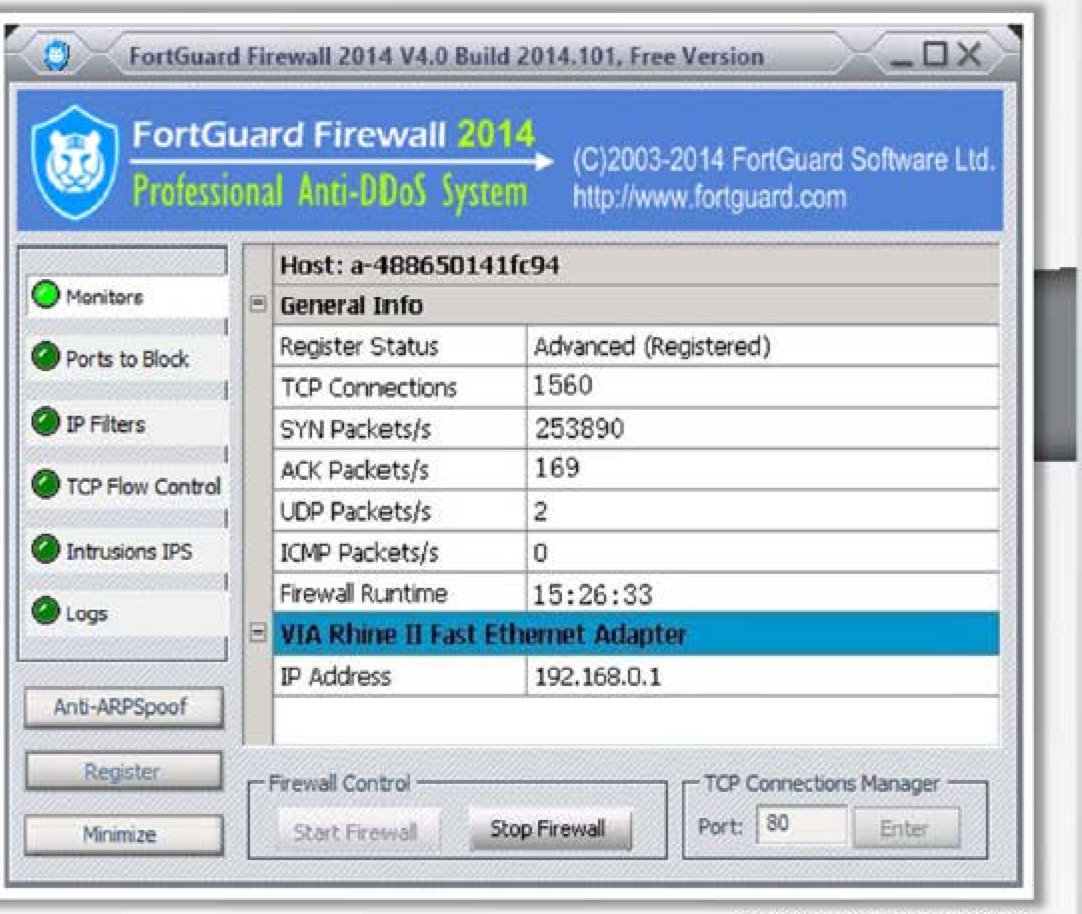
8 DoS/DDoS Penetration Testing

# 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



FortGuard Firewall 2014 V4.0 Build 2014.101, Free Version

FortGuard Firewall 2014

Professional Anti-DDoS System

(C)2003-2014 FortGuard Software Ltd.
http://www.fortguard.com

| Host: a-488650141fc94 | |
|---|---|
| **General Info** | |
| Register Status | Advanced (Registered) |
| TCP Connections | 1560 |
| SYN Packets/s | 253890 |
| ACK Packets/s | 169 |
| UDP Packets/s | 2 |
| ICMP Packets/s | 0 |
| Firewall Runtime | 15:26:33 |
| **VIA Rhine II Fast Ethernet Adapter** | |
| IP Address | 192.168.0.1 |

TCP Connections Manager — Port: 80

http://www.fortguard.com

# DoS/DDoS Protection Tools

**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

C|EH Certified Ethical Hacker

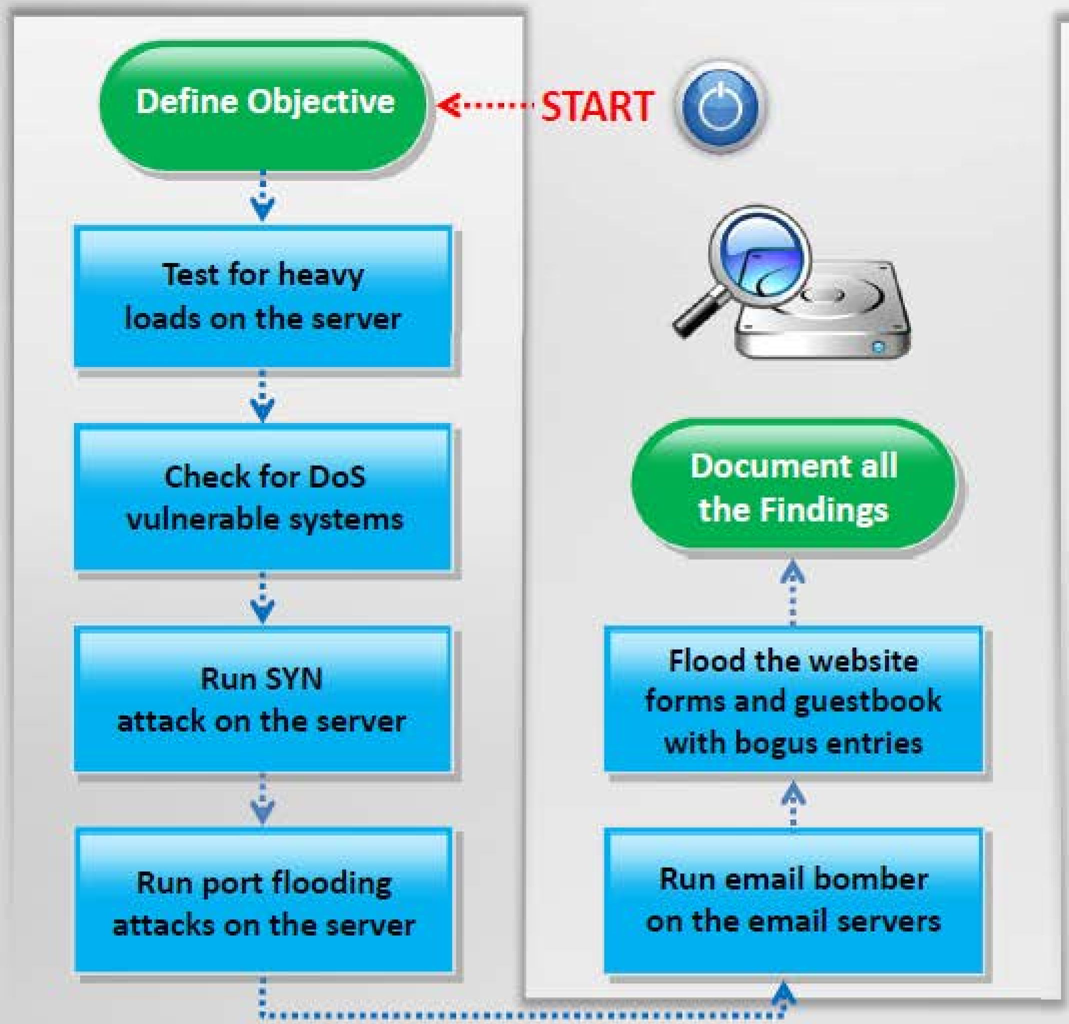
1. DoS attack should be incorporated into Pen testing plans to find out if the **network server** is susceptible to DoS attacks

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)



START

Define Objective

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

Run email bomber on the email servers

Flood the website forms and guestbook with bogus entries

Document all the Findings

- 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 Moihack 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