



# Sicurezza dei Dati

## Le Botnet

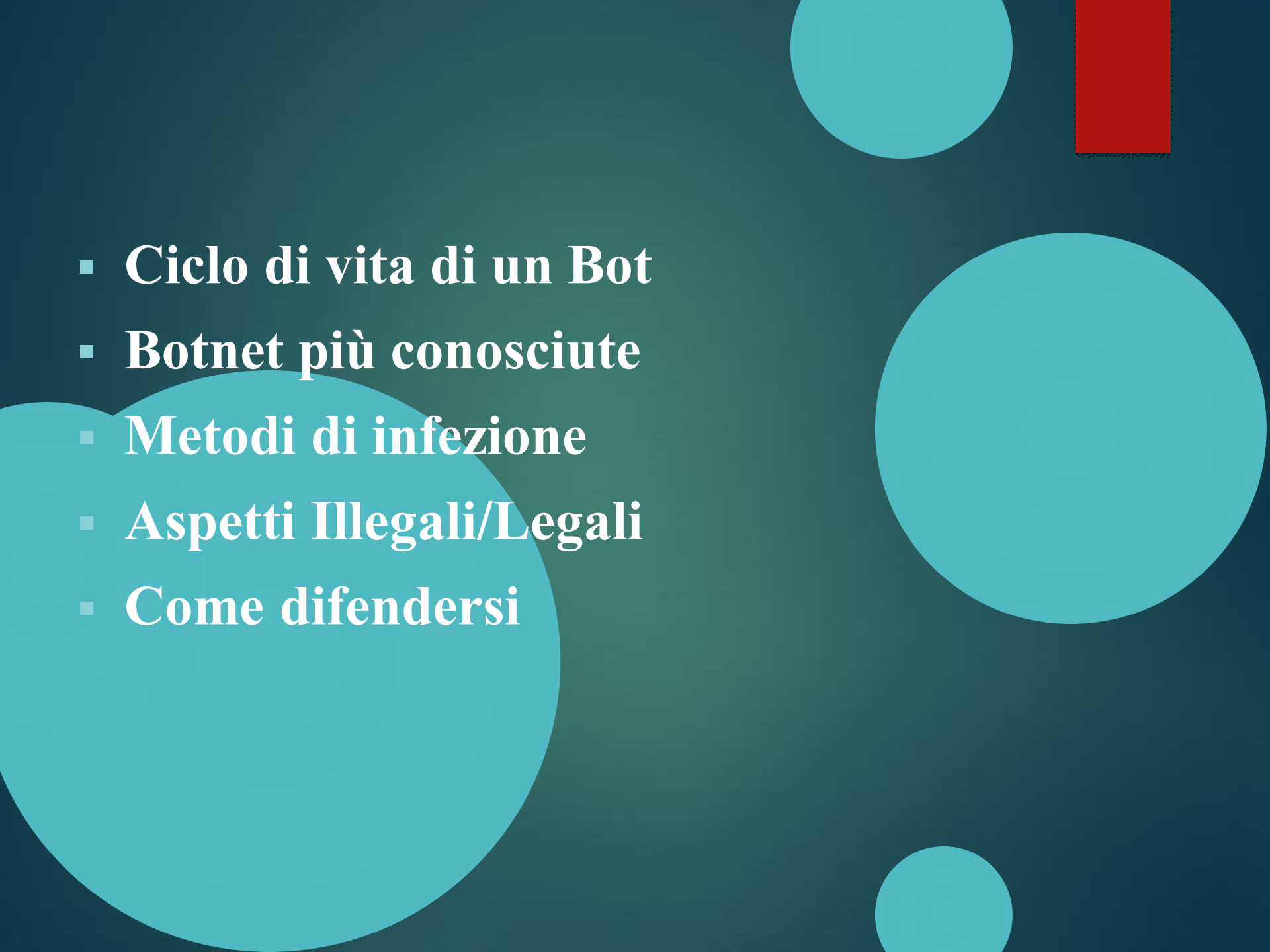


**Docente:**  
**Alfredo De Santis**

**Candidato:**  
**Giacomo Coccozzello**

# Indice

- **Introduzione**
- **Cos'è una Botnet**
- **Struttura di una Botnet**
- **Architettura**
- **Cos'è un bot/zombie**
- **Tipi di Bot**

- 
- The background is a dark teal gradient. It features several large, semi-transparent teal circles of varying sizes. A solid red vertical rectangle is positioned in the upper right corner. The text is white and arranged in a bulleted list on the left side of the slide.
- **Ciclo di vita di un Bot**
  - **Botnet più conosciute**
  - **Metodi di infezione**
  - **Aspetti Illegali/Legali**
  - **Come difendersi**

# Introduzione

Negli ultimi anni si sta diffondendo il fenomeno della Internet of Things dove oggetti d'uso comune si connettono in rete.

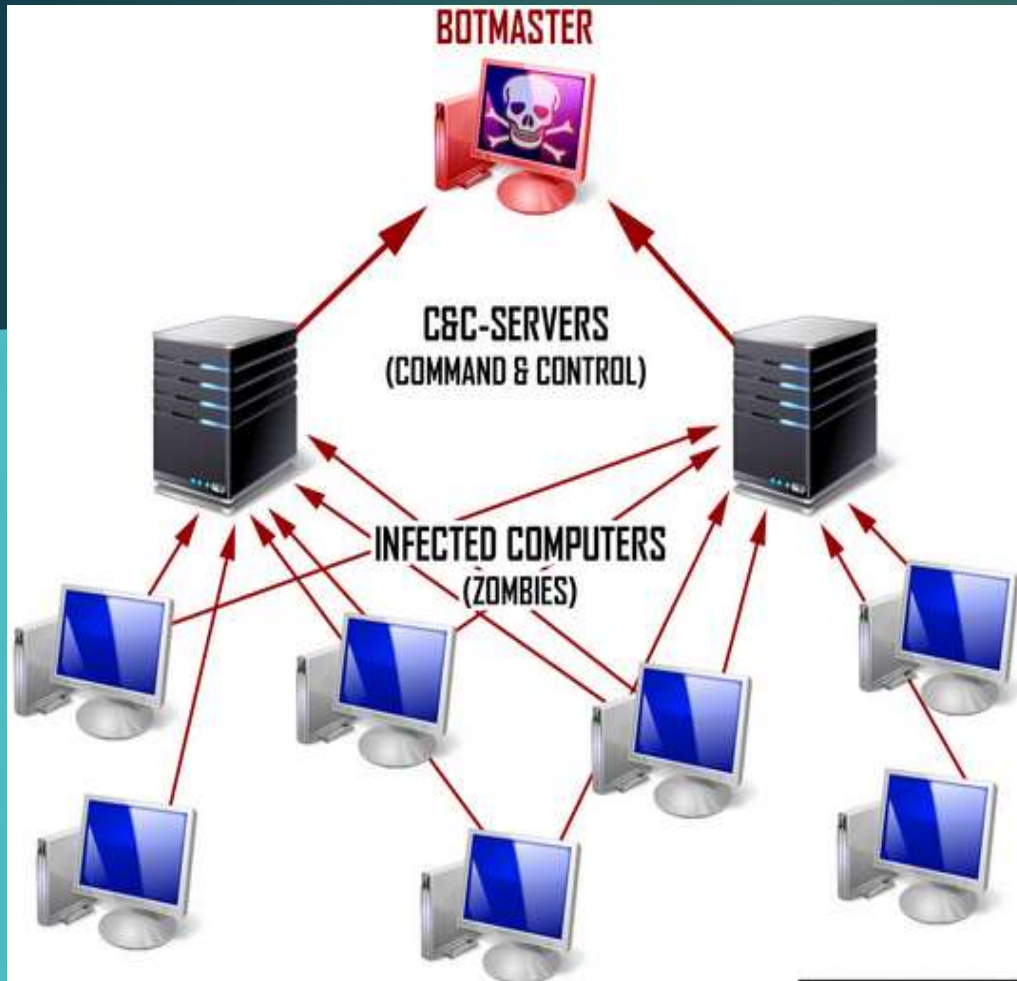


# Cos'è una Botnet?

Botnet deriva dalla parola roBOT NETwork, ovvero una rete di bot o anche detti computer zombie.



# Struttura di una Botnet



- Botmaster
- Unità di Comando e Controllo(C&C)
- Canale di Comunicazione
- Zombie(Bot)

# Botmaster

- ▶ È la persona o il gruppo di persone che si occupano di controllare i bots remoti.
- ▶ Ha il compito di progettare e scrivere malware per infettare i dispositivi.
- ▶ Riesce inoltre a non essere identificato dagli altri computer presenti nella rete.

# Unità di Comando e Controllo

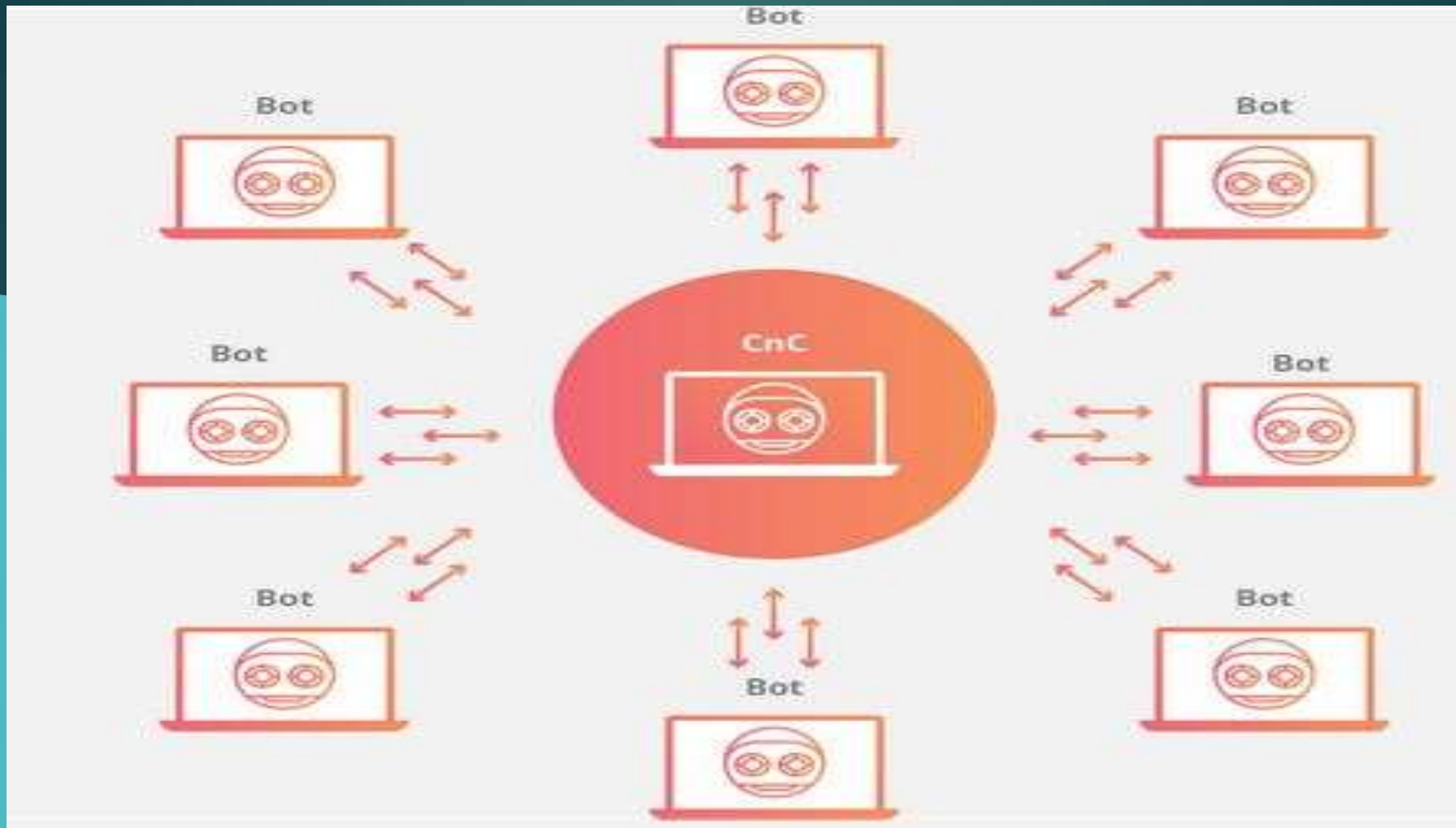
- ▶ Allertare gli zombie della Botnet
- ▶ Inoltrare gli ordini del Botmaster ai computer infettati.
- ▶ Schermare il Botmaster affinché non sia rintracciabile all'interno della rete.



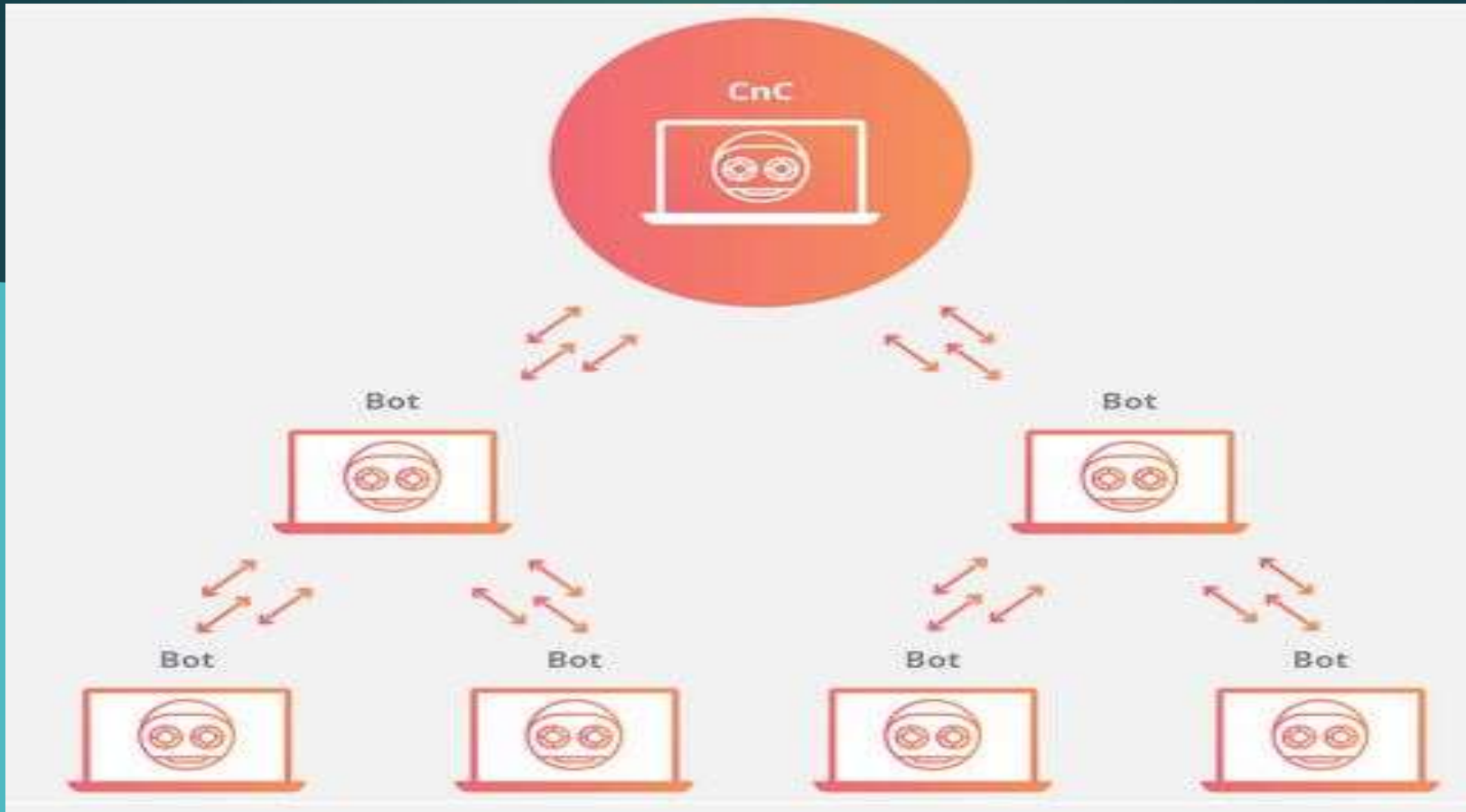
# Architettura Botnet

- ▶ **Botnet Centralizzate**
- ▶ **Botnet Gerarchiche**
- ▶ **Botnet Decentralizzate**

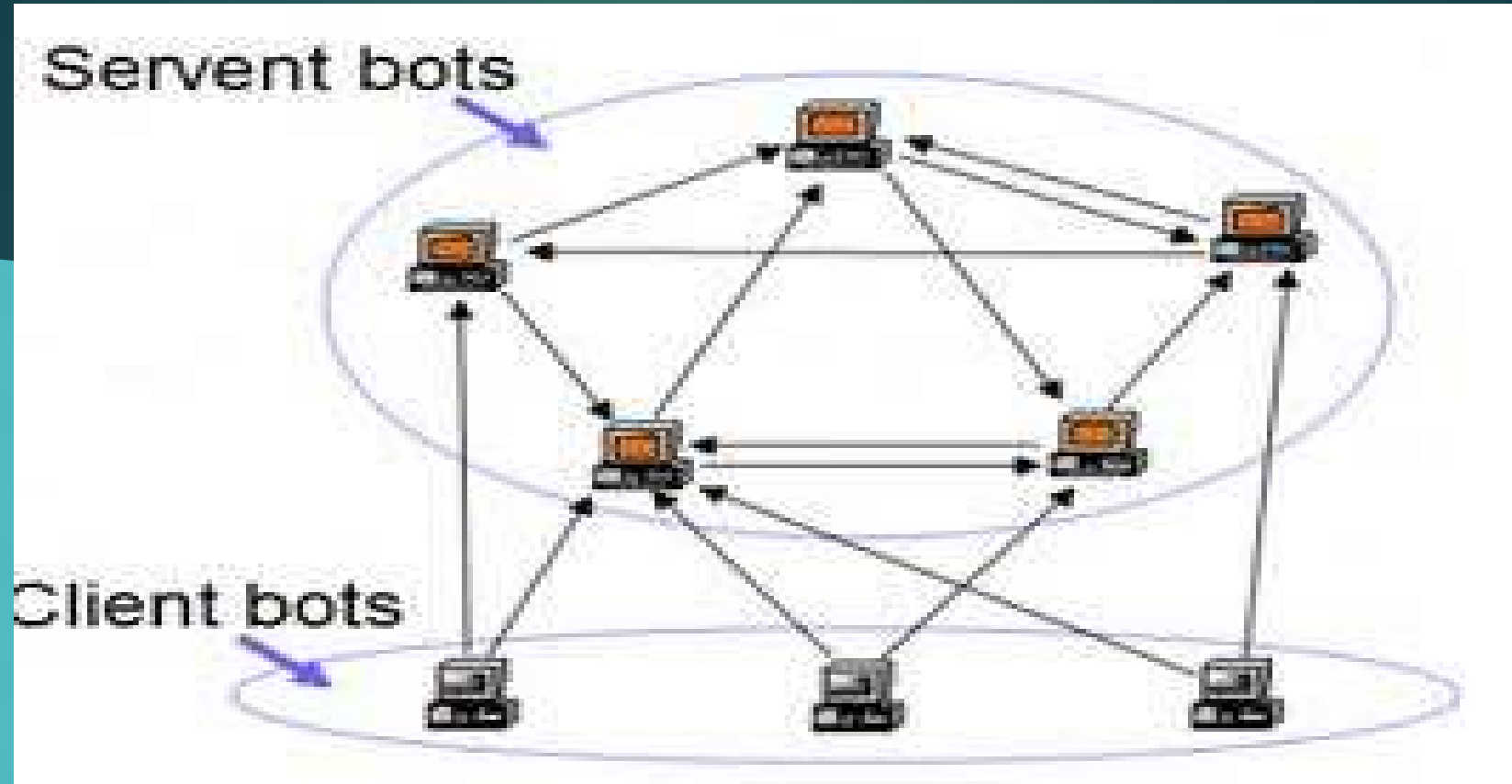
# Botnet Centralizzate



# Botnet Gerarchie



# Botnet Decentralizzate



# Botnet Centralizzate

Fanno uso dei seguenti canali di comunicazione:

- ▶ **IRC:** è la più classica interfaccia di controllo, la più antica forma di chat online e quella più amata dagli hacker.
- ▶ **HTTP:** è un mezzo di comunicazione più scomodo dell'IRC, ma ha il vantaggio che il traffico non viene filtrato dai firewall.
- ▶ **P2P:** I Botmaster potrebbero nascondere i bot tra i file comuni e riuscire ad installare i programmi che hanno il compito di infettare.

# Botnet Decentralizzate

Fanno uso dei seguenti canali di comunicazione:

- ▶ **IM Oriented:** per rendere più facili le comunicazioni alcuni bot comunicano tramite servizi di messaggistica istantanea.
- ▶ **Web-Service:** utilizzano servizi web diffusi (pastebin, gmail) come server C&C.

# Cos'è un Bot/Zombie

- ▶ Indica sia il computer infettato che il malware che è stato utilizzato per infettarlo.
- ▶ Utilizzato per compiere attacchi verso terze parti, attraverso spam o DDoS.

# Tipi di Bot

► Agobot

► SDBot

► Kaiten

► DSNX



# Agobot

- ▶ È il bot più conosciuto al momento.
- ▶ Scritto in C++ per agevolare la portabilità tra le diverse piattaforme
- ▶ Utilizza LIBPCAP
- ▶ Utilizza un protocollo di controllo diverso da IRC

# SDBot

- ▶ Scritto in C
- ▶ Largamente utilizzato in Internet
- ▶ Design meno astratto di Agobot
- ▶ Insieme semplificato di comandi

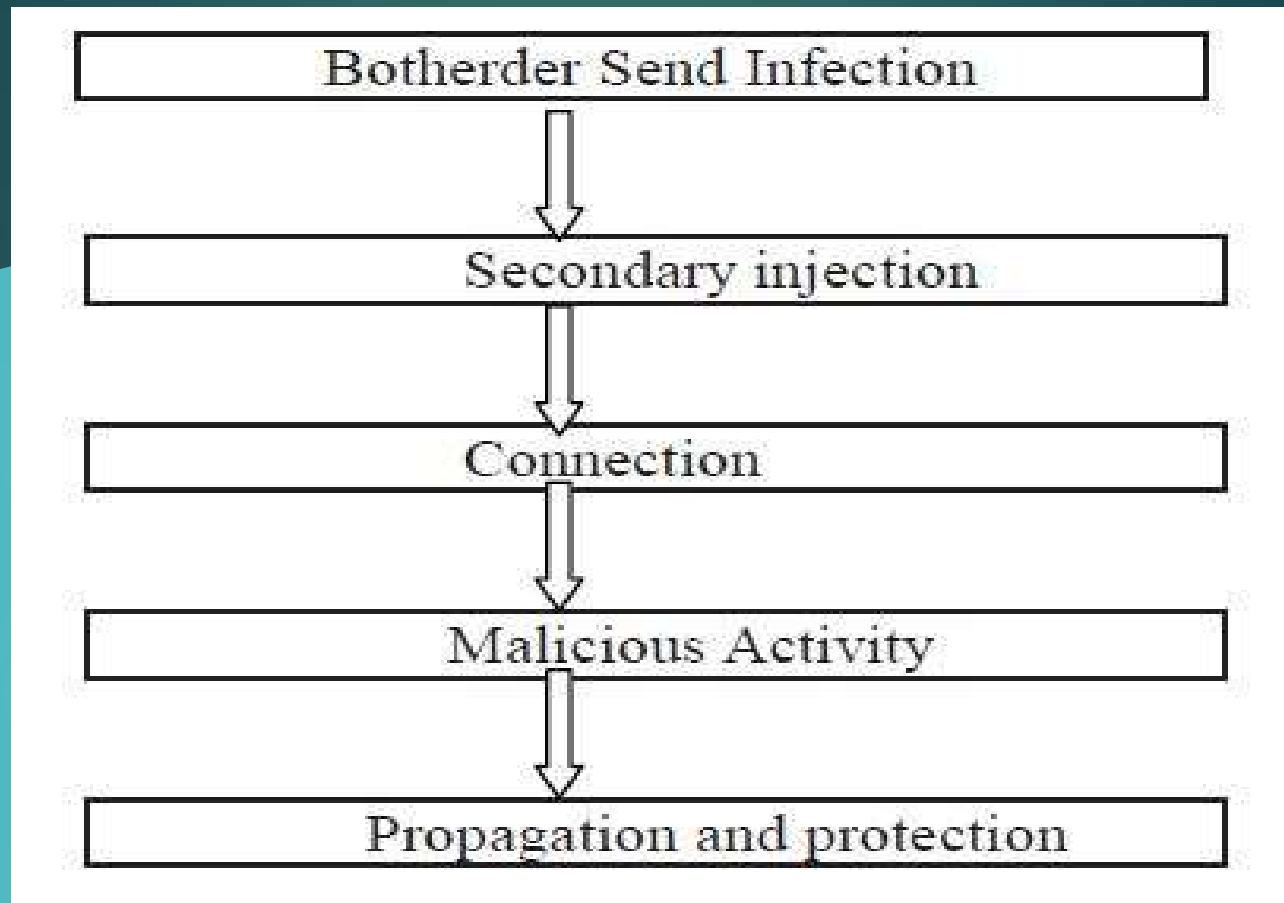
# Kaiten

- ▶ Progettato per attaccare sistemi Linux
- ▶ Dotato di una remote shell che permette all'hacker di ricercare le altre vulnerabilità del sistema infettato.

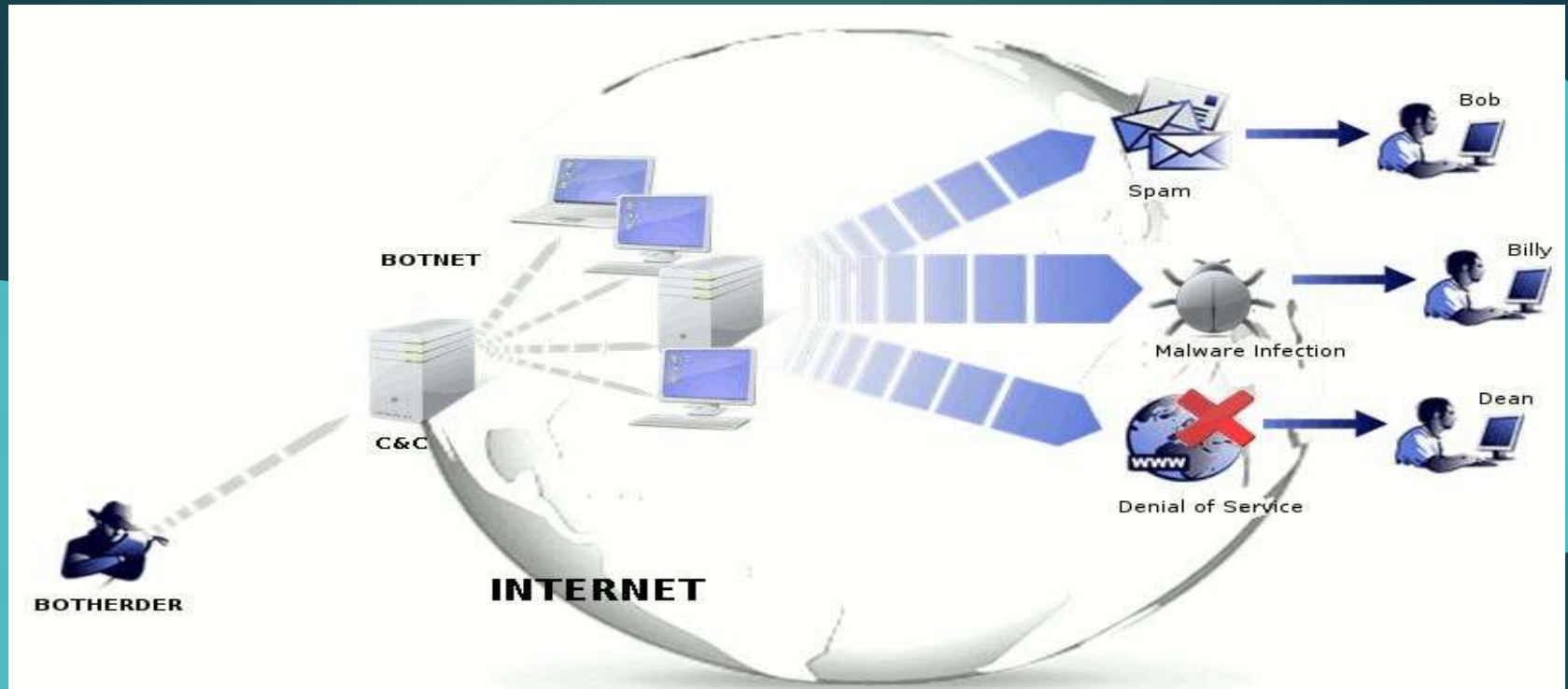
# DSNX

- ▶ **Data Spy Network X è scritto in C++.**
- ▶ **Si basa su un'architettura a plug-in che permette l'aggiunta di funzionalità senza modificare la struttura principale.**
- ▶ **Dotato di alcuni plug-in che permettono attacchi DDoS oppure la creazione di server HTTP che dovranno ospitare siti maligni.**

# Ciclo di vita di un Bot



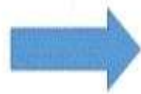
# Metodi di Infezione



# Drive-by download



Attacker does research on intended targets and sites they visit most



Attacker finds a vulnerable website and infects it with malware



When user visits the site the malware downloads onto user's machine

# Email

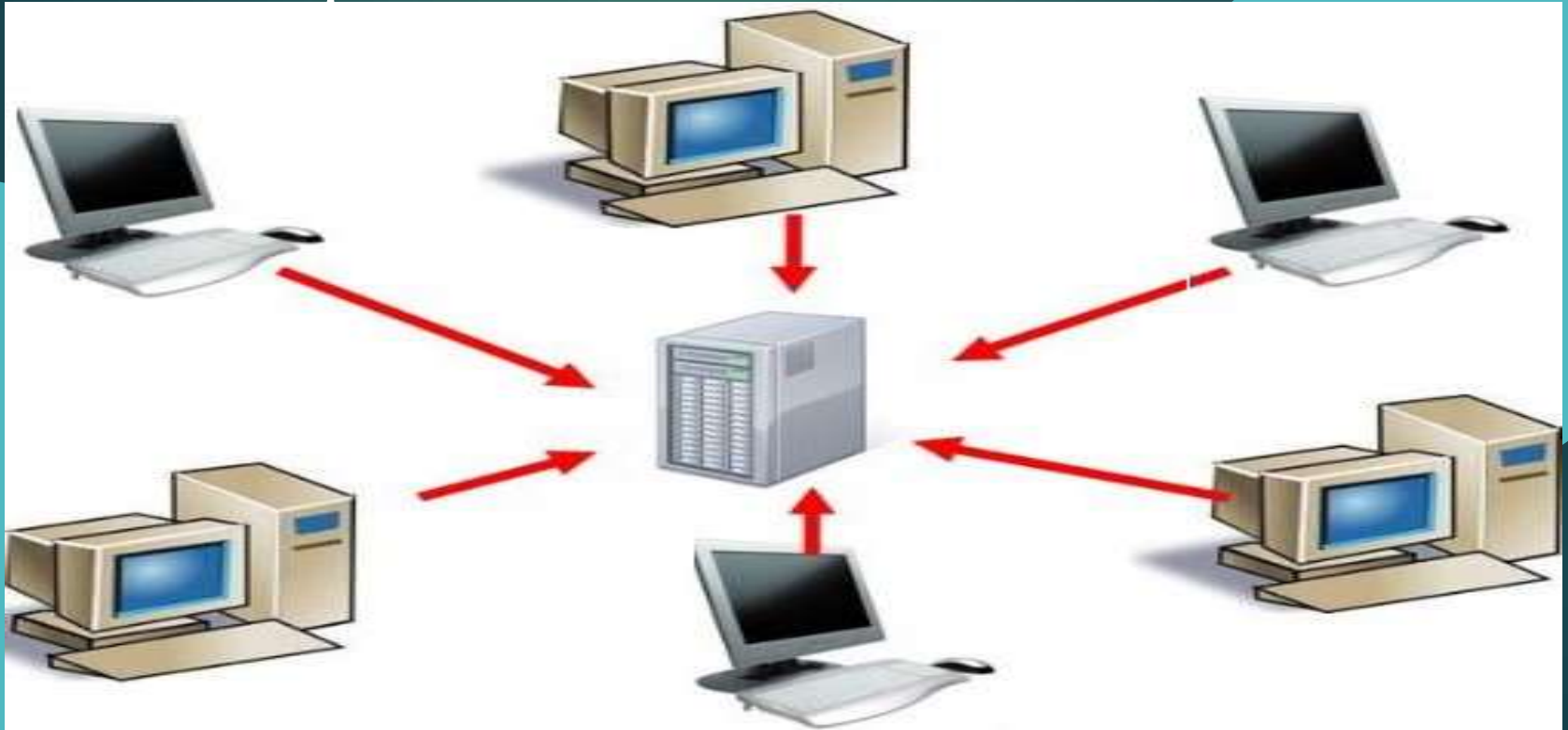
L'attaccante invia una grande quantità di email- spam con allegati contenenti file word o pdf con codici infetti o con link che reindirizzano l'utente ad un sito web che ospita il codice dannoso.





# Denial of Service(DoS)

**Blocca le risorse di un sistema informatico che fornisce un determinato servizio ai computer connessi.**



# Botnet più conosciute

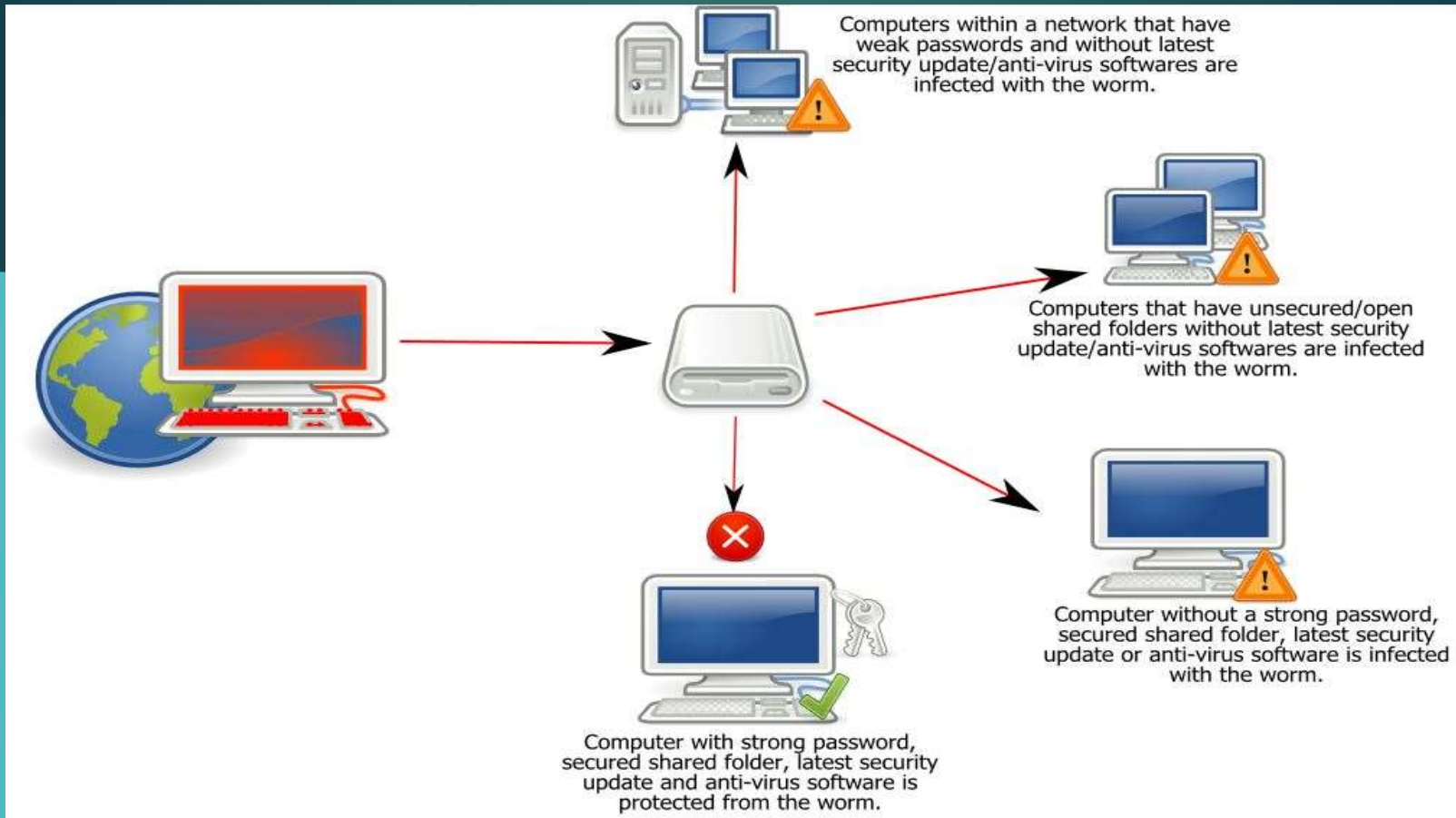
- ▶ **Conflicker**

- ▶ **Cutwail**

- ▶ **FlusiHoc**

- ▶ **Mirai**

# Confliker



# Cutwail

- ▶ È stata usata per inviare e-mail spam
- ▶ È stato stimato che è in grado di inviare 74 miliardi di e-mail spam al giorno

# Flusihoc

- ▶ **Botnet DDoS cinese**

- ▶ **Stringhe di bug**

  - “C:\Users\chengzhen\Desktop\svchost\Release\svchost.pdb”

- ▶ **il server C&C utilizza una struttura di comando basata sui numeri**

- ▶ **il bot utilizza un comando associato al numero del server.**



**I seguenti comandi individuati sono:**

**1 Richiede al bot di inviare informazioni sul sistema infettato ( S.O. – CPU – RAM)**

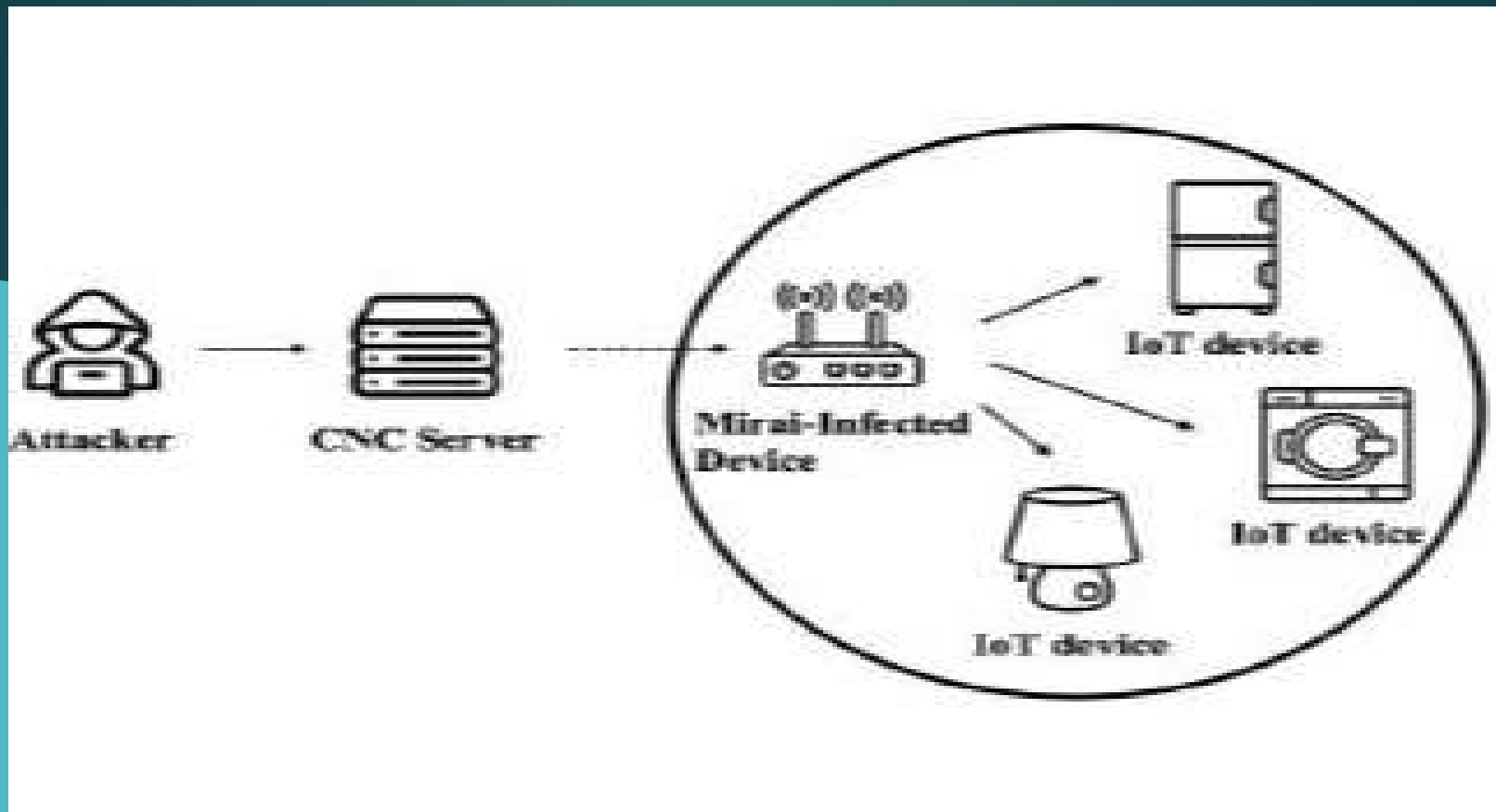
**4444 Comanda al bot di interrompere l'attacco in corso**

# Analisi Flusihoc

## DDoS Events Since July 2017

<b>Total Number of Events</b>	<b>909</b>
<b>Average Number of Attacks/Day</b>	<b>14.66 Attacks</b>
<b>Peak Attack Size</b>	<b>45.08 Gbps</b>
<b>Average Attack Size</b>	<b>603.24 Mbps</b>

# Mirai

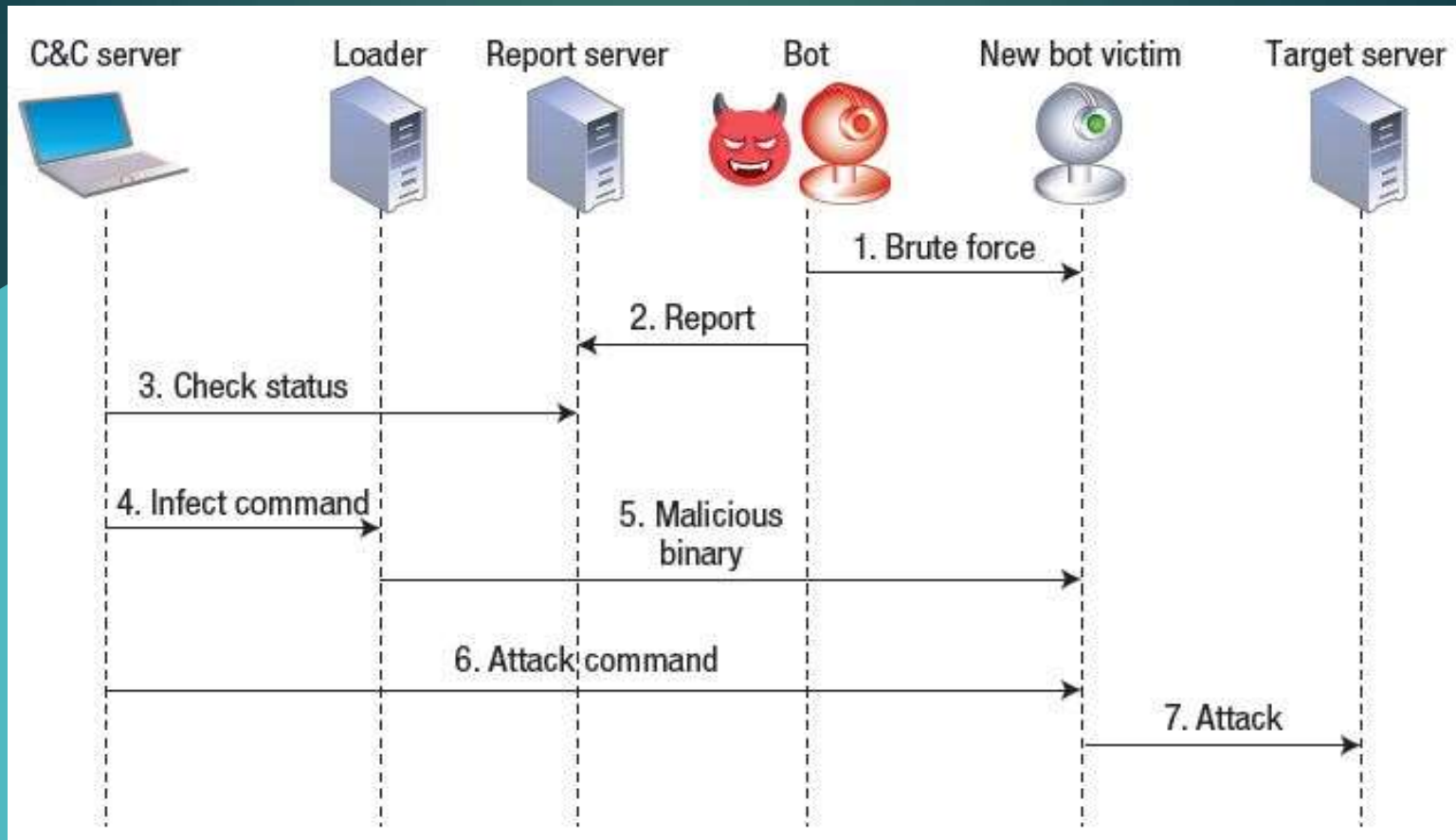




# Componenti Mirai

- Bot
- Target Server
- Server (C&C)
- Loader
- Report Server

# Funzionamento Mirai



# Mirai Attacchi

➤ Livello di applicazione

➤ Livello di rete

# Aspetti Illegali /Aspetti Legali

- ▶ Studio/Analisi sul calcolo distribuito
- ▶ Studio sulla diffusione del malware

# Come difendersi

► **Prevenzione**

► **Identificazione**

► **Risposta**

# Prevenzione

- **Mantenere il S.O. sempre aggiornato**
- **Gestione sicura di mail, browser**
- **Usare e aggiornare costantemente l'antivirus**
- **Firewall sempre attivo sull'host connesso in rete**

# Identificazione

- **Alto traffico sulla porta 6667**
- **Eccessivo ritardo nelle risposte dalla rete**
- **Utilizzare risorse online che ispezionano il sistema**

# Risposta

- **Disconnettere ogni dispositivo connesso in rete**
- **Aggiornare l'antivirus e aggiornare le patch del S.O.**
- **Cambiare le password dei dispositivi attaccati**



# Conclusioni

- ▶ **Moltiplicazione esponenziale dei dati raccolti**
- ▶ **Aumento indiscriminato dei malintenzionati**
- ▶ **Intrinseca insicurezza dei dispositivi IoT**
- ▶ **Assenza di regole per le aziende che producono dispositivi IoT**

# Bibliografia

- ✓ **DDoS in the IoT: Mirai and other Botnets.pdf**
- ✓ **Understanding Botnet on Internet.pdf**
- ✓ **Botnets: The Anatomy of case.pdf**
- ✓ **Botnets Threat Analysis and Detection.pdf**
- ✓ **Understanding the Mirai Botnet.pdf**
- ✓ **Botnets – the killer web applications(libro)**
- ✓ **Botnets and Internet of Things Security**
- ✓ **Botnet - <http://www.antibot.it/it/content/cosa-sono-le-botnet>**

**Grazie per l'attenzione!**

