Corso di Sicurezza su Reti 2

Le Botnet

Docente: Alfredo de Santis

Studente: di Chiara Gabriele

Outline

- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una Botnet
- Infiltrarsi in una Botnet
- Botnet più conosciute
- Difendersi dalle Botnet

Nuovi attacchi alla rete

- Hacking di applicazioni web
- Phishing
- Vishing
- Botnets/FastFlux

Hacking applicazioni Web

- Analisi di web application fatta per individuare le vulnerabilità di un sistema per ottenere dati che verranno utilizzati dal pirata informatico per le sue frodi informatiche. Tali vulnerabilità vengono sfruttate tramite diverse tecniche come:
    - Cookie Poisoning
    - Hidden field
    - Parameter Tampering
    - SQL Injection
    - XSS

Phishing

- Principalmente utilizzata per carpire informazioni sensibili e/o personali (es. numero di carta di credito).
- Viene inviata una mail agli utenti contenente avvisi di situazioni pendenti particolari da regolarizzare urgentemente.
- L’utente viene indirizzato da questa verso una copia fittizia del sito ufficiale e in cui inserire i suoi dati personali.
- Queste informazioni vengono memorizzate, e successivamente usate, dal phisher per acquistare beni, trasferire somme di denaro o si può anche usare l'utente come "ponte" per attacchi a sistemi ad esso connessi.

Vishing (Frodi su VoIP)

- Termine derivato dalla fusione di V(oIP) e (Ph)ishing.
- Attacco portato a sistemi di messaggistica istantanea oppure a programmi di VoIP (es. Skype).
- Più semplici da eseguire con successo rispetto a quelli fatti sull'email, essendo utenti meno sensibilizzati sui rischi che l'utilizzo di tale mezzo comporta.
- Tali attacchi vengono effettuati tramite chiamate vocali o messaggi preregistrati per sottrarre informazioni sensibili, quali codici di carte di credito o informazioni personali.

Perdite causate dalle frodi online

	Stima	Fonte
Frodi online di banche del Regno Unito (6/2007–5/2008)	£36.5 milioni	APACS (2008)
Perdite dirette dovute a furto di identità negli U.S.A. (2006)	$2.8 miliardi	Gartner (2006)
Danni in Europa causati dal malware (2006)	€9.3 miliardi	Computer Economics (2007)

Il Nemico

Outline

- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una Botnet
- Infiltrarsi in una Botnet
- Botnet più conosciute
- Difendersi dalle Botnet

Cos'è un Bot (Zombie)

- Abbreviazione di “robot”
- Si riferisce sia al malware usato per creare la rete di computer zombie e sia ai computer contaminati che fanno parte della rete.
- Tali computer obbediscono agli ordini che vengono loro impartiti da colui che controlla la rete.
- **Definizione:** *un gruppo di computer controllati da una singola sorgente ed esegue programmi e script collegati al software (http://www.techterms.com/)*

Cos'è una Botnet

- Una Botnet è una rete di computer Bot.
- Viene creata tramite un programma, progettato dall'hacker che vuole controllare tali computer. Dopo l'invio, viene eseguito automaticamente sui computer attaccati.
- L'aggressore, spesso difficilmente rintracciabile e sempre nascosto all'interno della rete, riesce ad assumere il controllo dei computer colpiti facendoli diventare suoi succubi.

Perché creare una Botnet ?

Per dimostrare la propria abilità nel penetrare le difese dei computer.

L'affare delle Botnet

- Inizialmente usate con il solo scopo di inondare la rete con enormi quantità di messaggi di spam.
- Successivamente sfruttate dalle aziende, che utilizzando un sito web per il proprio commercio, volevano abbattere i siti concorrenti e risultare più visibili.
- **Attenzione:** Non bisogna considerarsi protetti dalla contaminazione solo perché il proprio PC non appartiene ad una rete commerciale.

Stime pc compromessi

	Stima	Fonte
Computer facenti parti di *botnet*	5 milioni	Symantec (2008)
Computer infetti con software maligno per furto di identità	10 milioni	Panda Security (2009)
False pagine web usate per il *phishing*	116.000	Moore and Clayton
Siti web che infettano i visitatori per mezzo di software maligno (*malware*)	3 milioni	Provos et al. (2008)

Come avviene la contaminazione

- Si introducono link in siti molto usati. Questi saranno utili al server pirata per penetrare nei PC da contaminare attraverso lo sfruttamento di falle di sicurezza contenute nel browser o in altri programmi presenti sull'host.
- Se l'attacco ha successo si assegna al PC vittima un codice per l'identificazione sulla rete; l'unica cosa visibile all'utente sarà: RIAVVIO IMPROVVISO DEL COMPUTER.
- Il Bot si va a posizionare in un settore di boot in modo da risultare invisibile agli antivirus. Si carica in memoria un file .DLL che agisce da backdoor.
- Il pirata riesce, attraverso l'uso di toolkit come Neosploit o Mpack, ad avere il totale controllo del nostro PC e inoltre a gestire tutti gli altri computer della rete, facendo così in modo di avere un esercito virtuale pronto ad eseguire gli ordini impartiti.

Anatomia di una Botnet

- Gli elementi di cui è costituita una Botnet sono:
  - Il Botmaster
  - Unità di Comando e Controllo
  - Canale di comunicazione
  - Zombie (Bot)

Botmaster

- Il Botmaster, conosciuto anche come BotHerder è la persona o il gruppo di persone che si è occupa di controllare i Bots remoti.
- Si trova in un luogo sicuro e molto lontano rispetto a quello dell'infezione, come accennato in precedenza.
- Riesce inoltre a non essere identificato dagli altri computer presenti nella rete grazie alla sua capacità di cambiare indirizzo IP più volte nell’arco della stessa giornata.

Unità di comando e controllo

- Centro di controllo di una Botnet.
- I compiti principali:
  - Allertare gli zombie della Botnet
  - Inoltrare gli ordini del master ai computer infettati
  - Schermare il Botmaster affinché non sia rintracciabile all'interno della rete

Tipologia C&C

- Le unità di Comando e Controllo possono utilizzare diversi canali di comunicazione e differenti modi di dialogare con i computer zombie della Botnet. Abbiamo quindi centri con:
  - **Controllo centralizzato (Push)**
  - **Controllo distribuito (Pull)**

Push VS Pull

- Le modalità di scambio di messaggi si distinguono per il modo di comunicare col server e si dividono in:
  - **Push**: tiene i bot in standby finchè il master non decide di allertarli per poi inviare loro un comando.
  - **Pull**: sono i bot che interrogano continuamente il master per sapere se ci sono nuovi ordini da svolgere.

Controllo Centralizzato

- Sicuramente il metodo di comunicazione più usato dalle prime Botnet.
- Fa uso dei seguenti canali di comunicazione:
  - **IRC**: è la più classica di interfaccia di controllo, la più antica forma di chat online, la più amata dagli hacker. I master utilizzano una chatroom con migliaia di utenti, che in realtà sono tutti gli zombie della sua rete. Un comando scritto in tale chat dal Botmaster ottiene un'immediata mobilitazione di migliaia di zombie.
  - **Http**: è un mezzo di comunicazione più scomodo rispetto a IRC, ma ha il fondamentale vantaggio che il traffico così generato non è filtrato dai firewall. Il Botmaster controlla tutte le caratteristiche della sua rete attraverso una pagina web da dove è in grado anche di ordinare gli attacchi.
  - **P2P**: rappresenta un nuovo mezzo di comunicazione sfruttabile dalle Botnet. Le reti basate su questo canale di comunicazione sfruttano la popolarità del p2p. Gli utenti potrebbero installare i Bot per errore, essendo questi spesso rinominati coi nomi dei file più scaricati.

Famiglie di Bot

- *XtremBot, Agobot, Forbot, Phatbot*
- *UrXBot, SDBot, UrBot e Rbot*
- *GT-Bots e Bots basati su mIRC*
- *DSNX*
- *Bot Q8*
- *Kaiten*
- *Bot in Perl*

XtremBot, Agobot, Forbot, Phatbot

- Sono i Bot più conosciuti al momento.
- Sono scritti in C++ per agevolare la portabilità tra le diverse piattaforme.
- Vengono rilasciati sotto GPL.
- Possono avere un design ad uno o più livelli, a seconda del livello di astrazione che si vuole garantire. Questo sicuramente per rendere più semplice l'aggiunta di nuove funzionalità al worm.
- *Gli Agobot* possiedono inoltre, vari meccanismi per nascondersi sulle macchine ospite e riescono a fare sniffing del traffico, identificando le versioni di Linux istallate sull'host.

UrXBot, SDBot, UrBot eRbot

- Rilasciato sotto GPL
- Sono scritti in C.
- Design meno astratto dei precedenti.
- Funzionalità offerte simili ad Agobot ma ha un insieme semplificato di comandi.
- Largamente utilizzati su Internet.

GT-Bots e Bots basati su mIRC

- Presente in molteplici versioni, essendo mIRC il più usato tra i client IRC per Windows.
- Si avviano sulla macchina vittima file binari tramite mIRC. Tali Bot si diffondono sfruttando le debolezze dei PC.
- Si possono facilmente estendere le funzionalità, tese a migliorare le tecniche di attacco, grazie ai moduli DLL.

DSNX

- Data Spy Network X è un client scritto in C++.
- È basato su un’architettura a plug-in che permette una facile aggiunta di funzionalità senza il bisogno di doverne intaccare la struttura principale.
- Alcuni plug-in disponibili sono quelli che permettono ad esempio l’attacco DDoS e la creazione di server HTTP che dovranno ospitare siti maligni.

Bot Q 8

- I più leggeri di questa categoria.
- Hanno un’orma molto piccola, grazie alle sole 926 linee di codice scritte in C++.
- Progettata principalmente per infettare sistemi Linux.
- Ha la capacità di auto aggiornarsi a versioni più recenti tramite download HTTP.

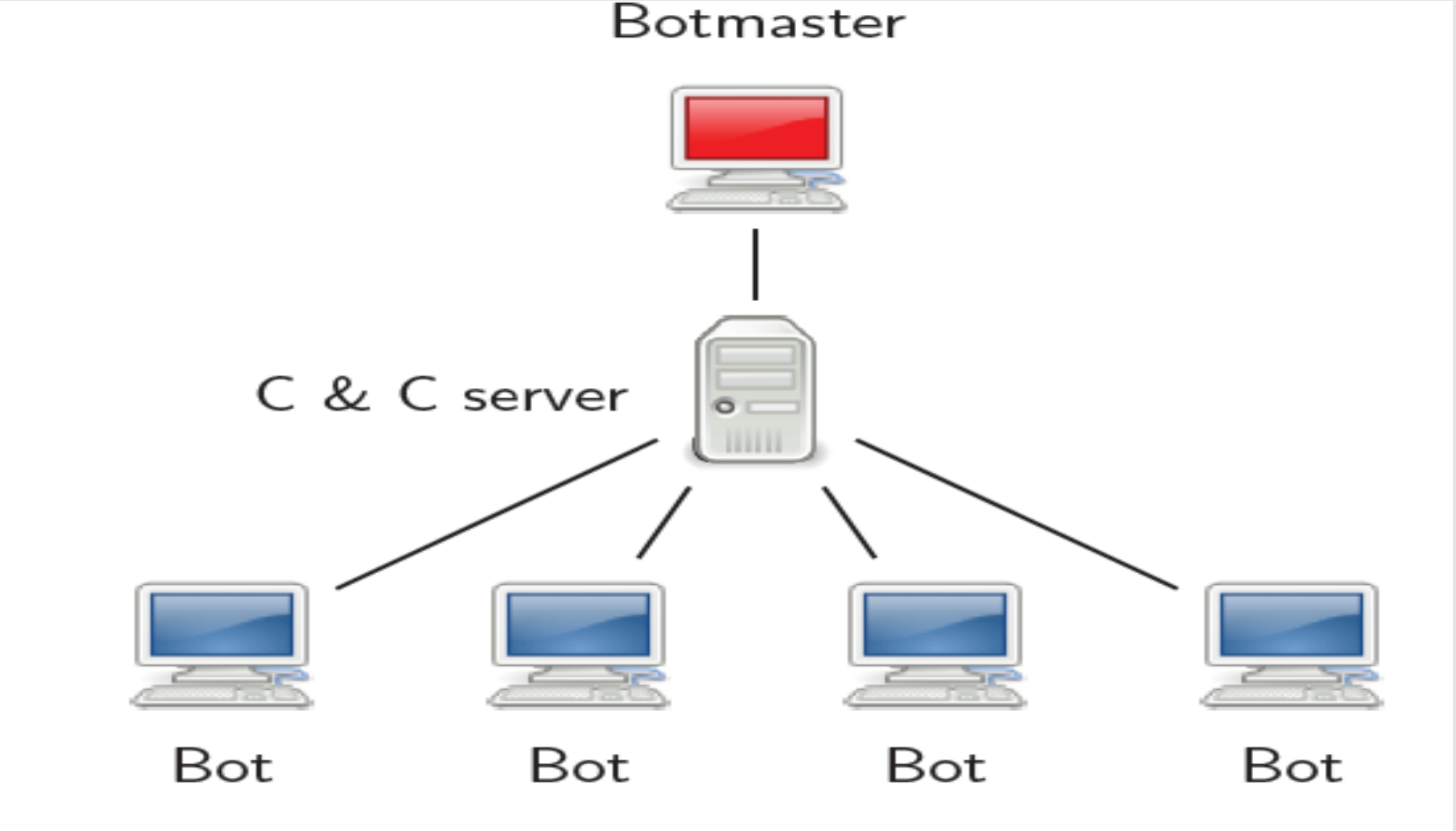
Kaiten

- Progettato per attaccare sistemi Linux e Unix.
- Dotato di una remote shell che permette all'hacker di ricercare le altre vulnerabilità del sistema infettato o di esplorarlo da remoto.
- Usato raramente a causa della debolezza del suo schema di autenticazione che è facilmente attaccabile dagli hacker.

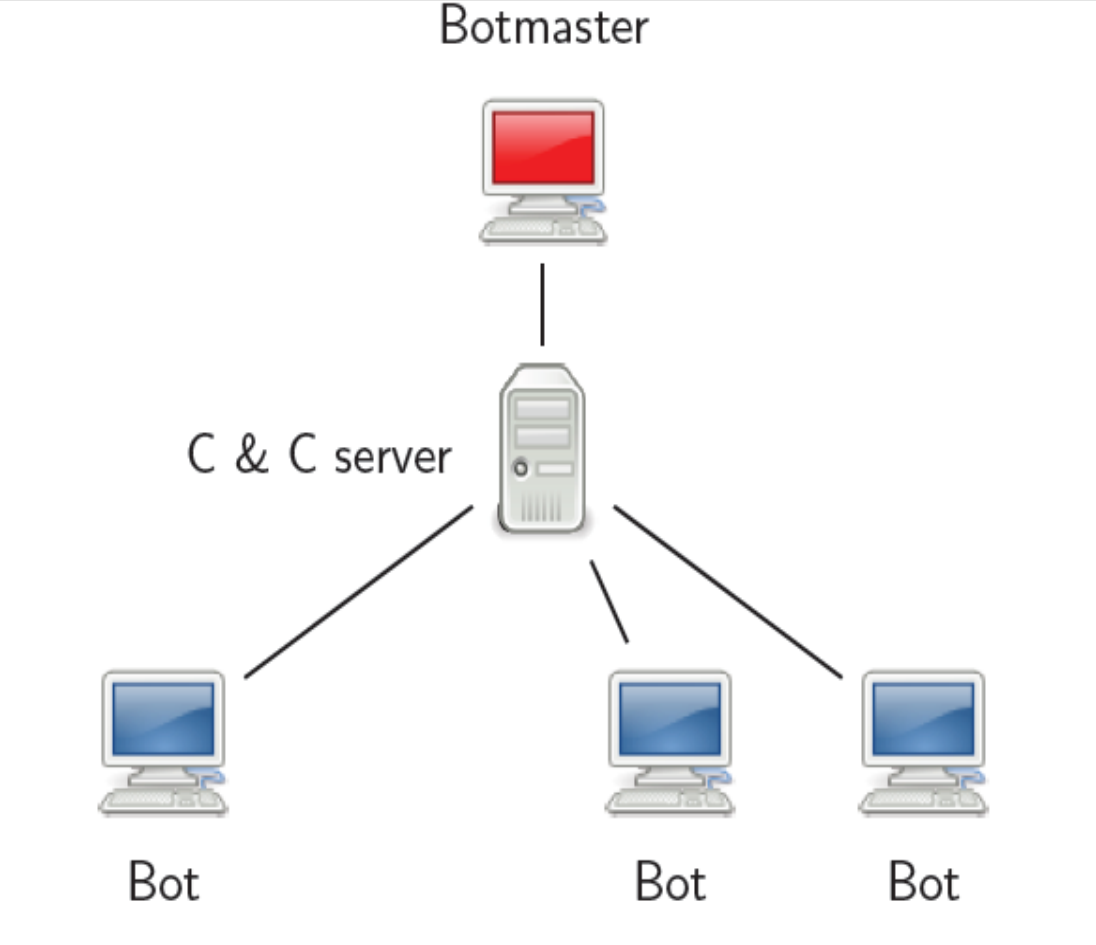
Bot in Perl

- Scritti in Perl
- Sono estremamente leggeri
- Offrono un insieme limitato di funzionalità all’hacker che li utilizza.
- Principalmente utilizzati per portare attacchi di tipo DDoS a sistemi Unix.

Struttura di una Botnet

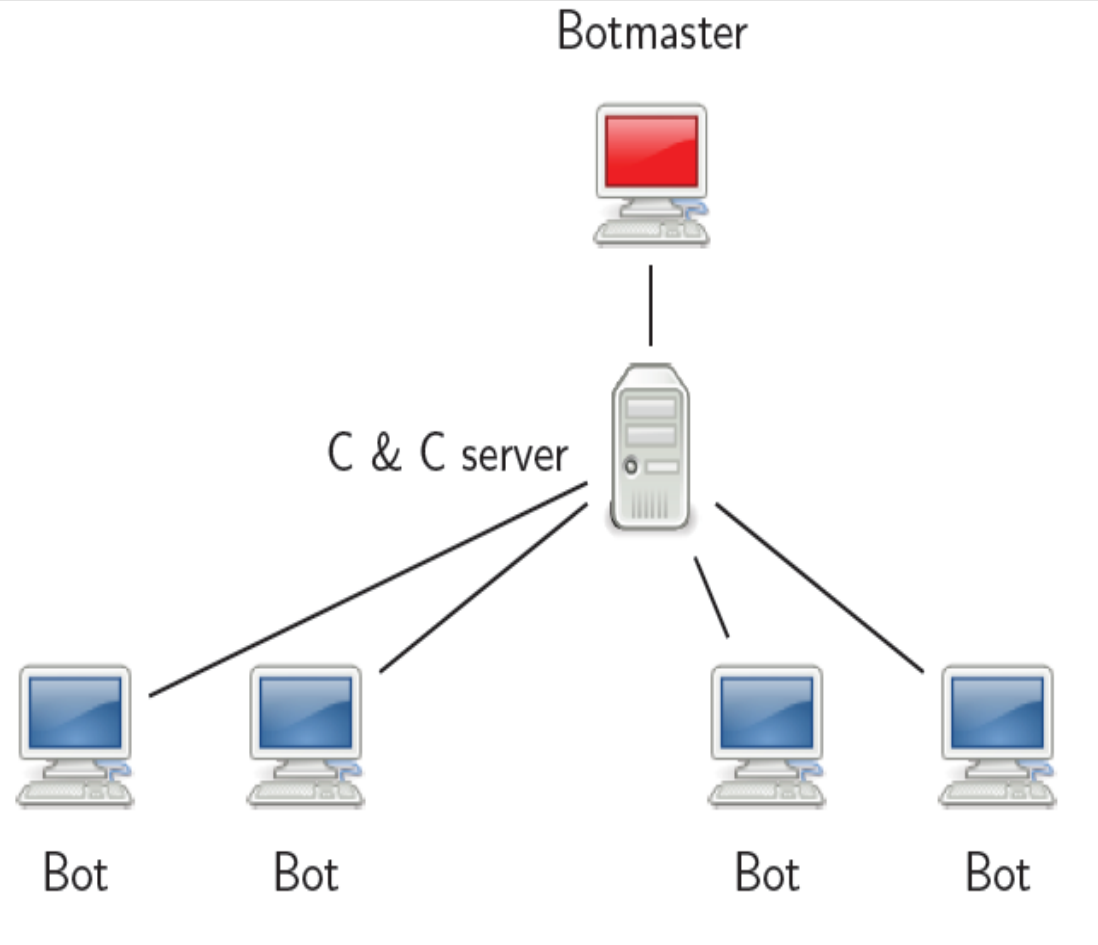


Funzionamento di una Botnet -1



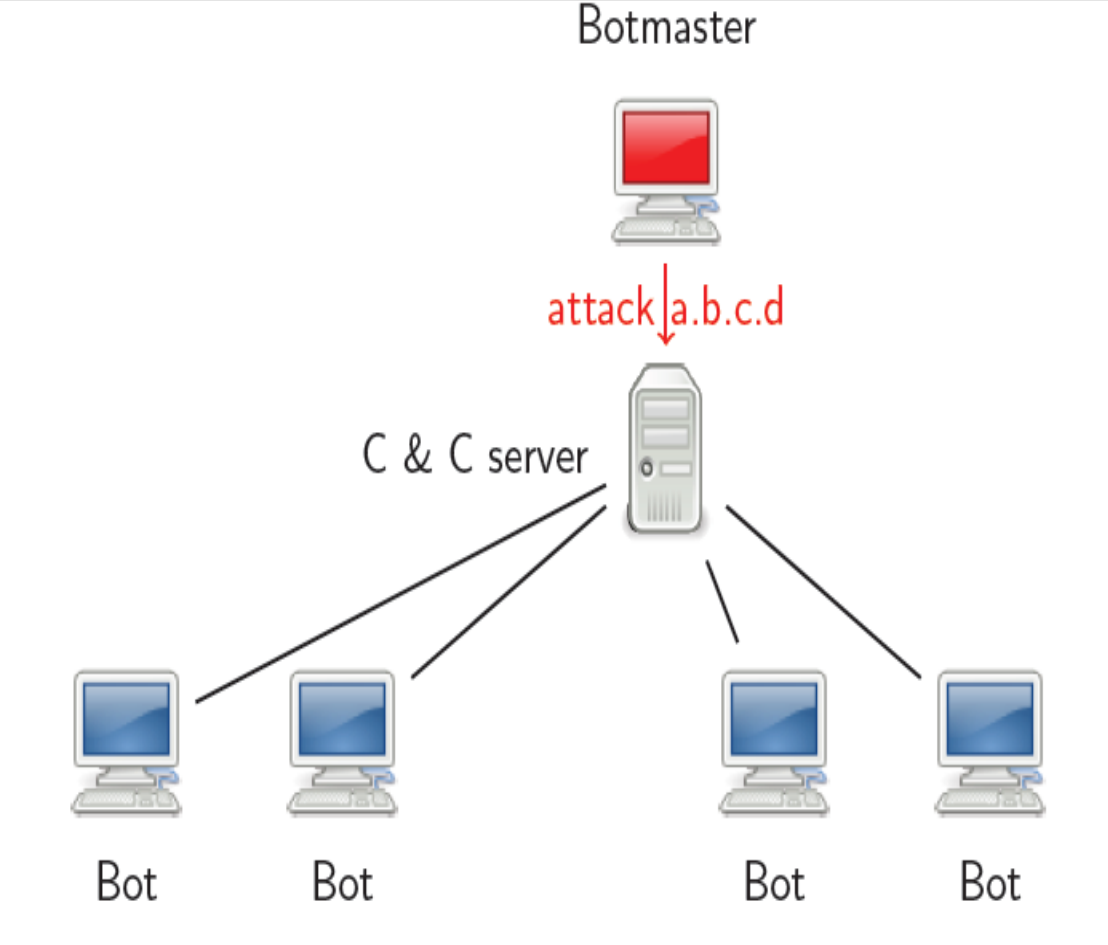
- I client che fanno parte di una Botnet si potrebbero connettere e disconnettere continuamente

Funzionamento di una Botnet -2



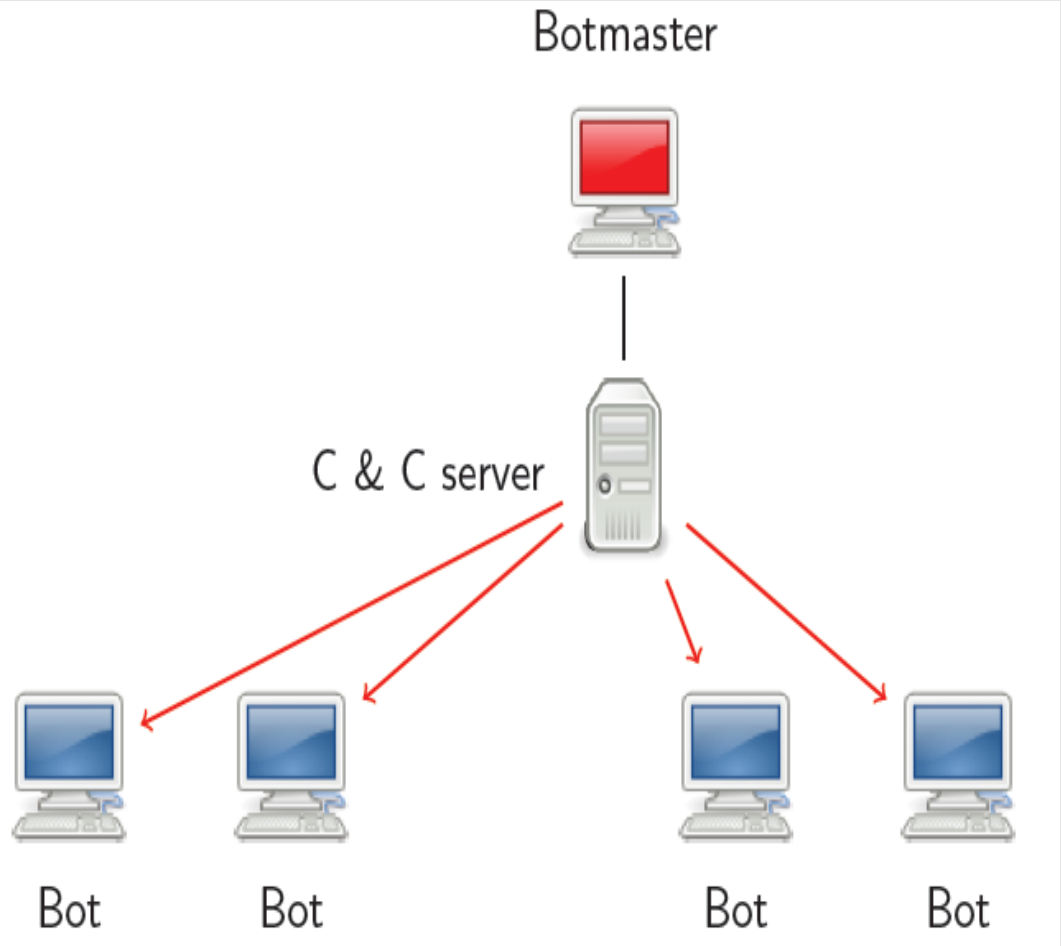
- I client che fanno parte di una Botnet si potrebbero connettere e disconnettere continuamente.

Funzionamento di una Botnet -3



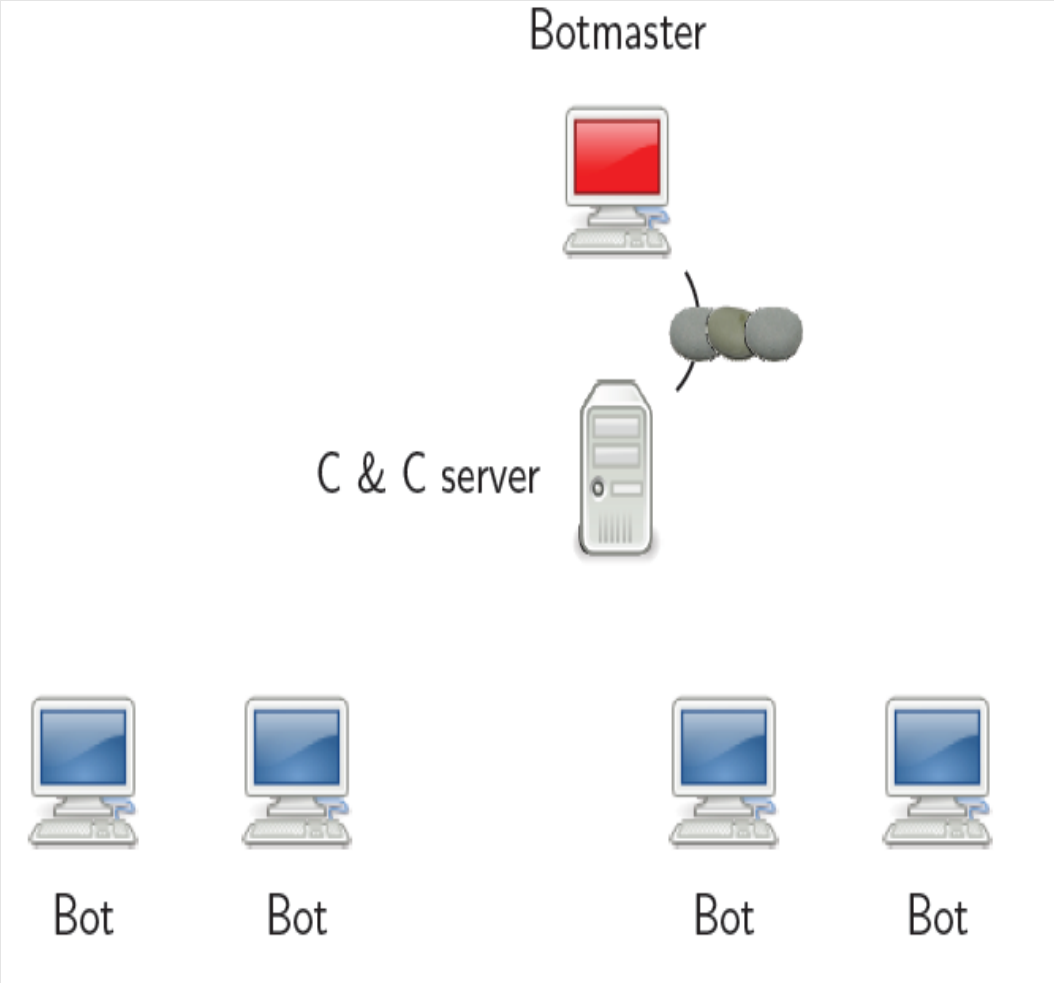
- Il Botmaster invia al C&C server il comando di attaccare i Bot.

Funzionamento di una Botnet -4



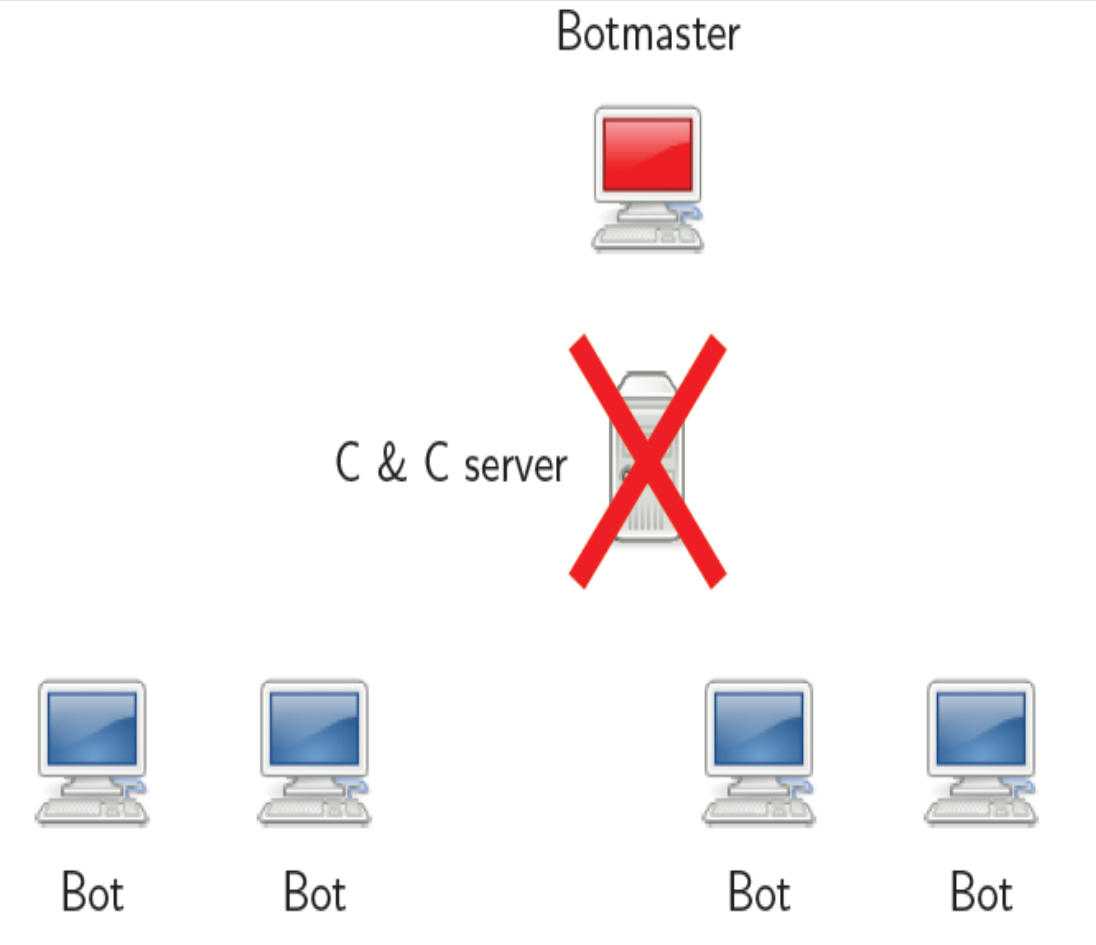
- Il C&C server inoltra tale comando a tutti i Bot connessi in quel momento.

Grande vantaggio



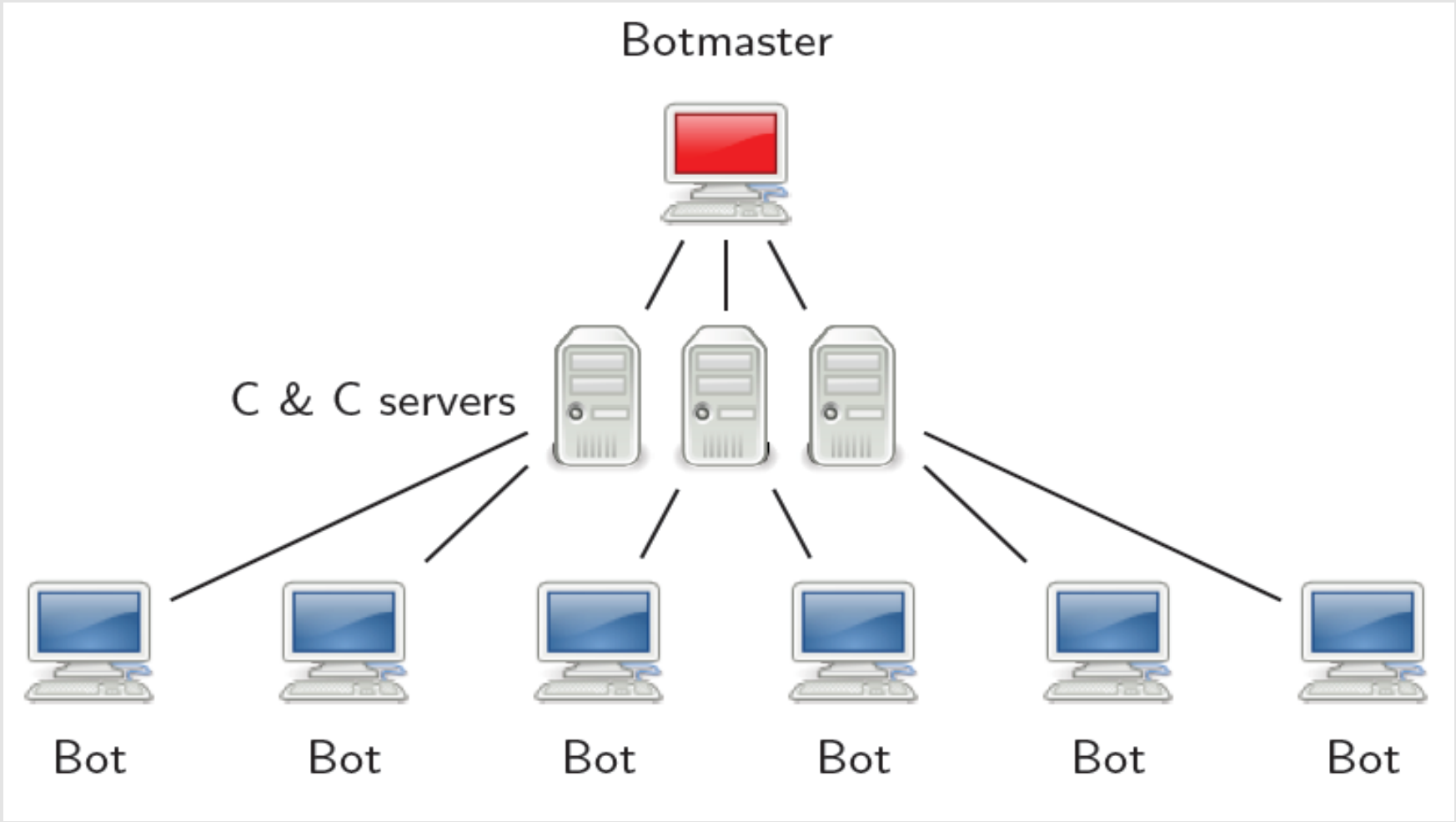
- Come detto in precedenza il server C&C rende il Botmaster difficilmente rintracciabile.

Svantaggio

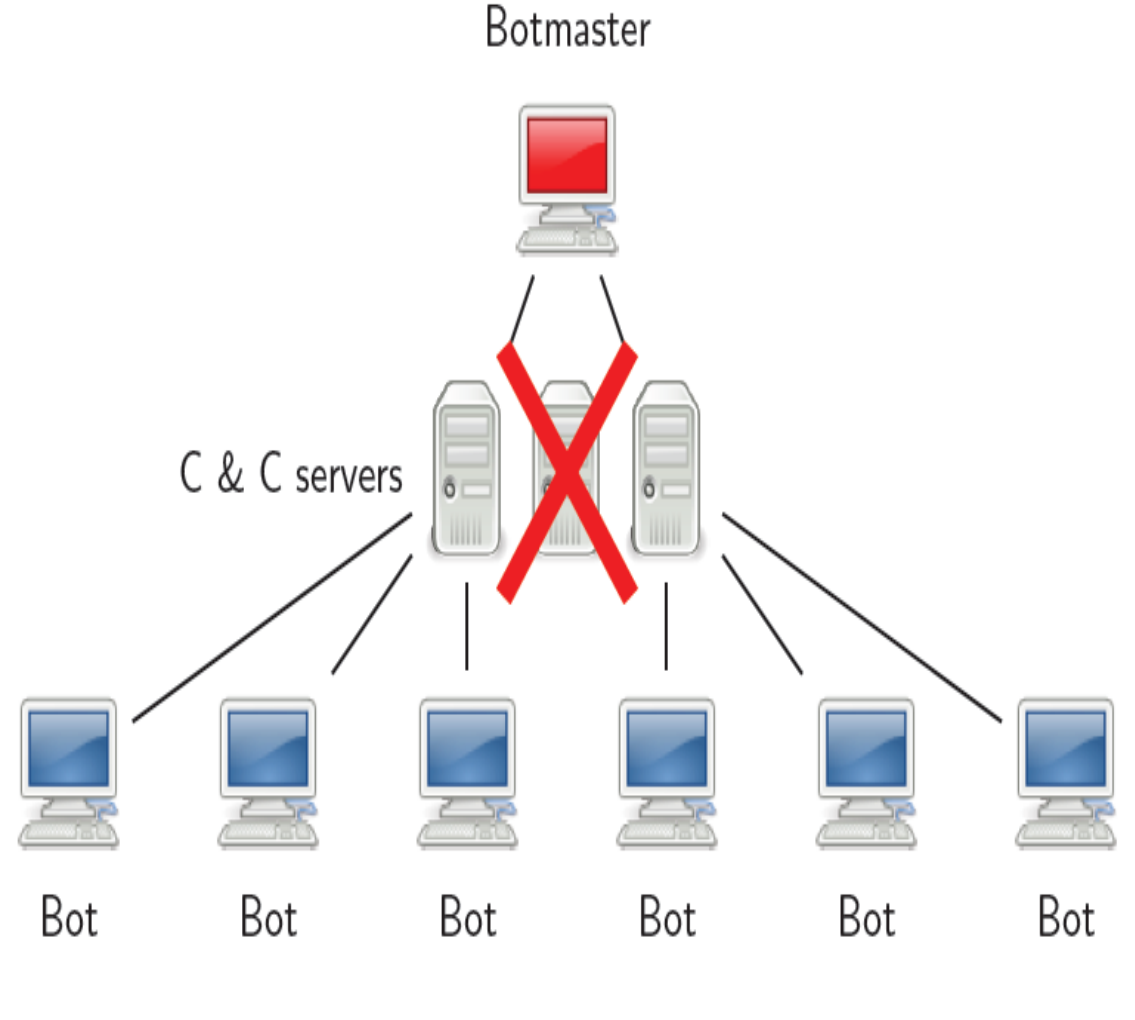


- Se il server C&C dovesse essere eliminato o danneggiato si perderebbe il controllo su tutti i bot della rete.

Soluzione: C&C server in Parallelo



C&C server in Parallelo -2

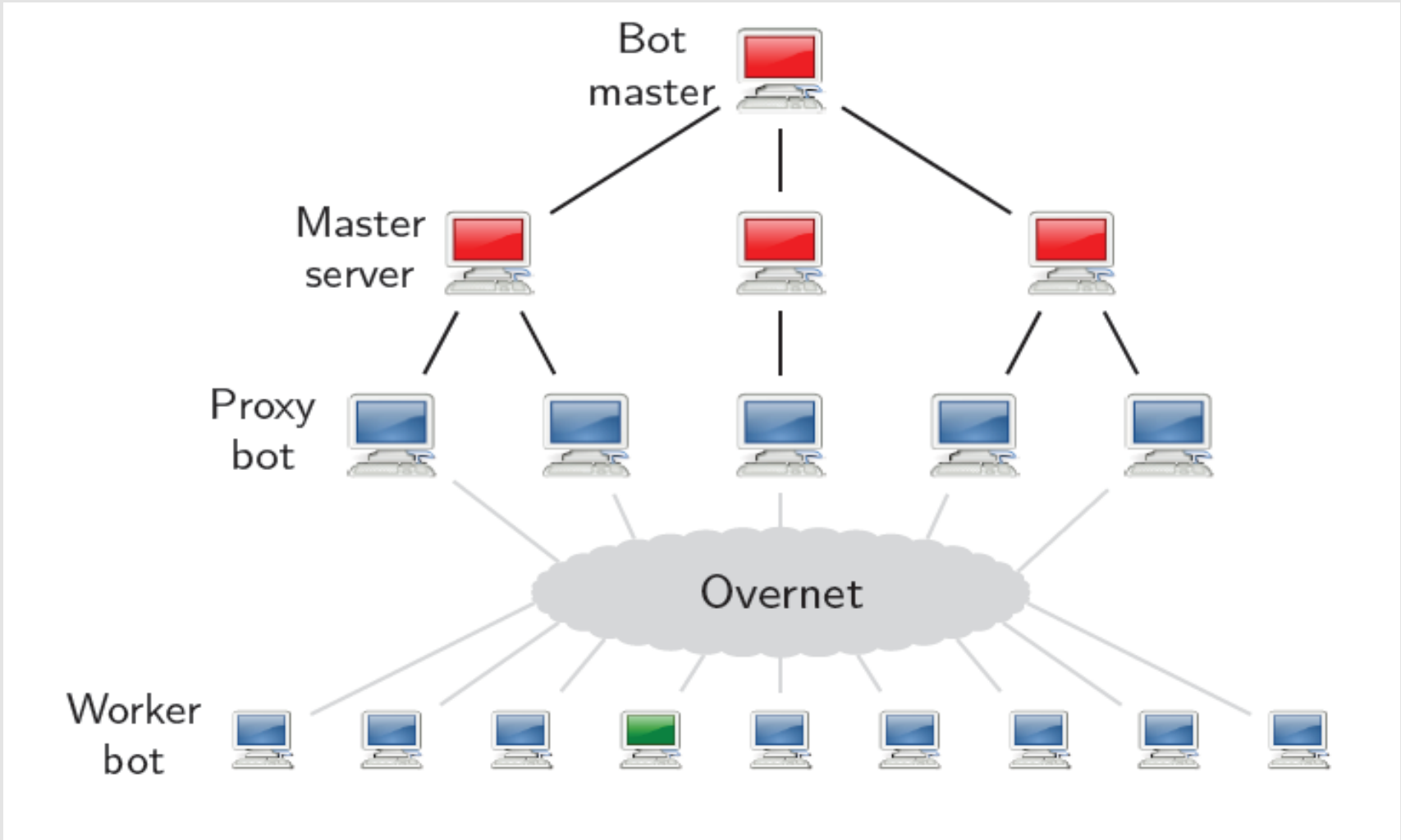


- Nel caso un server C&C venisse messo fuori uso i Bot che si collegavano ad esso si collegheranno automaticamente ai server ancora attivi.
- In questo modo anche la capacità della Botnet può essere incrementata.

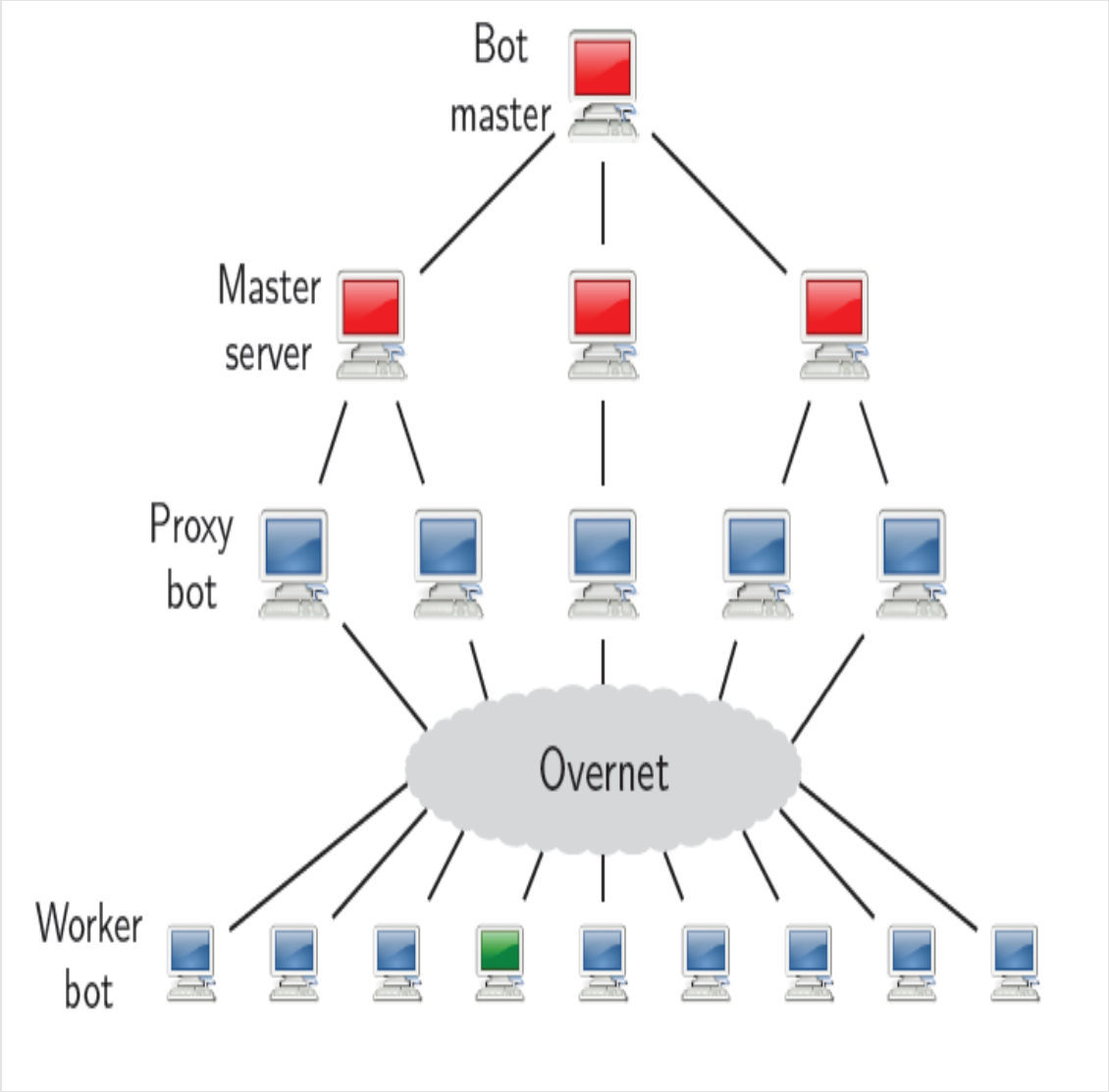
Botnet basate su HTTP

- Hanno la stessa struttura di quelle basate su IRC.
- Utilizzano modalità di comunicazione *pull.*
- Generano traffico facilmente confondibile con traffico benigno.
- Difficile da bloccare a livello di rete e di DNS.

Botnet basata su P2P

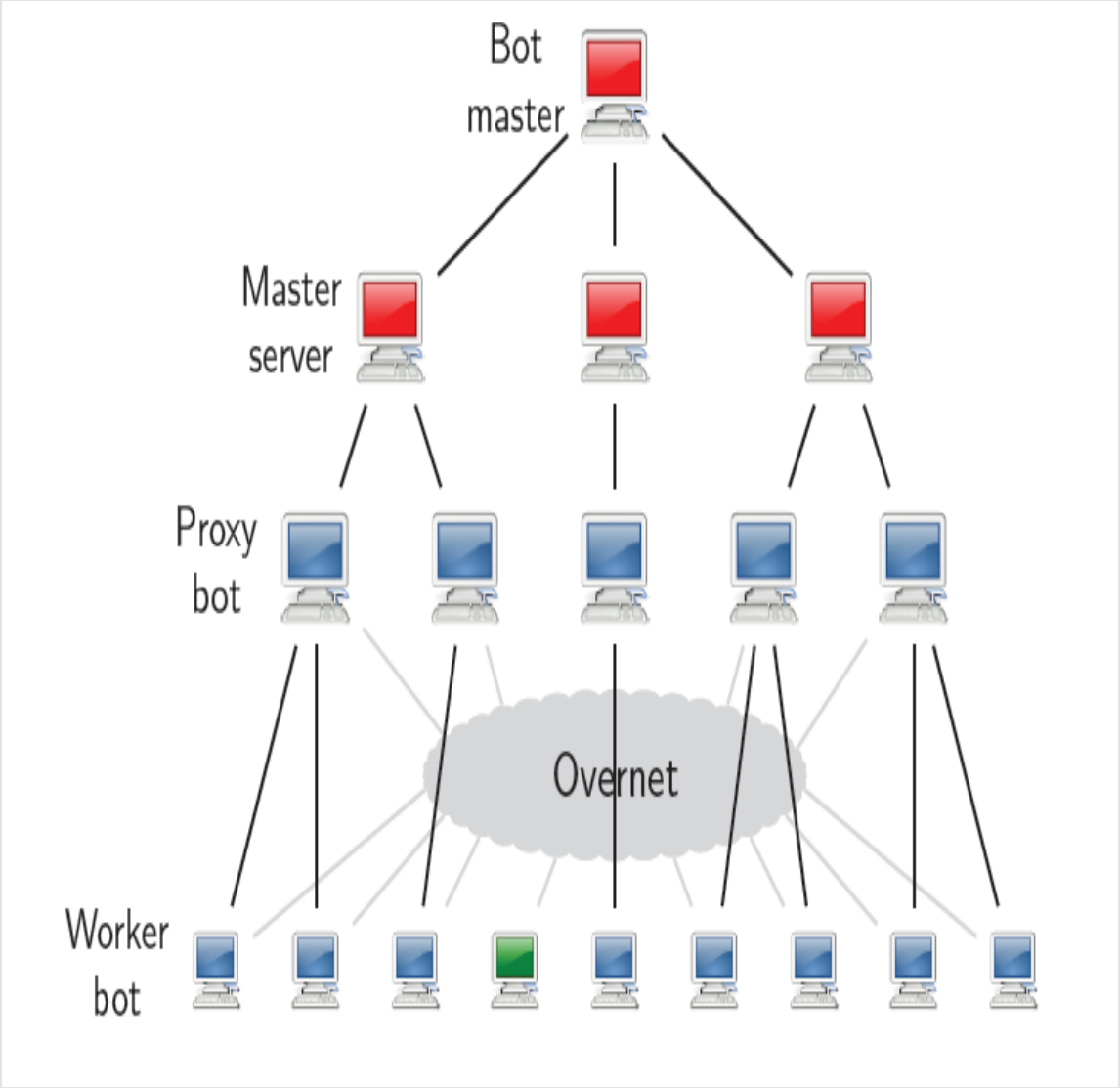


Botnet basata su P2P -2



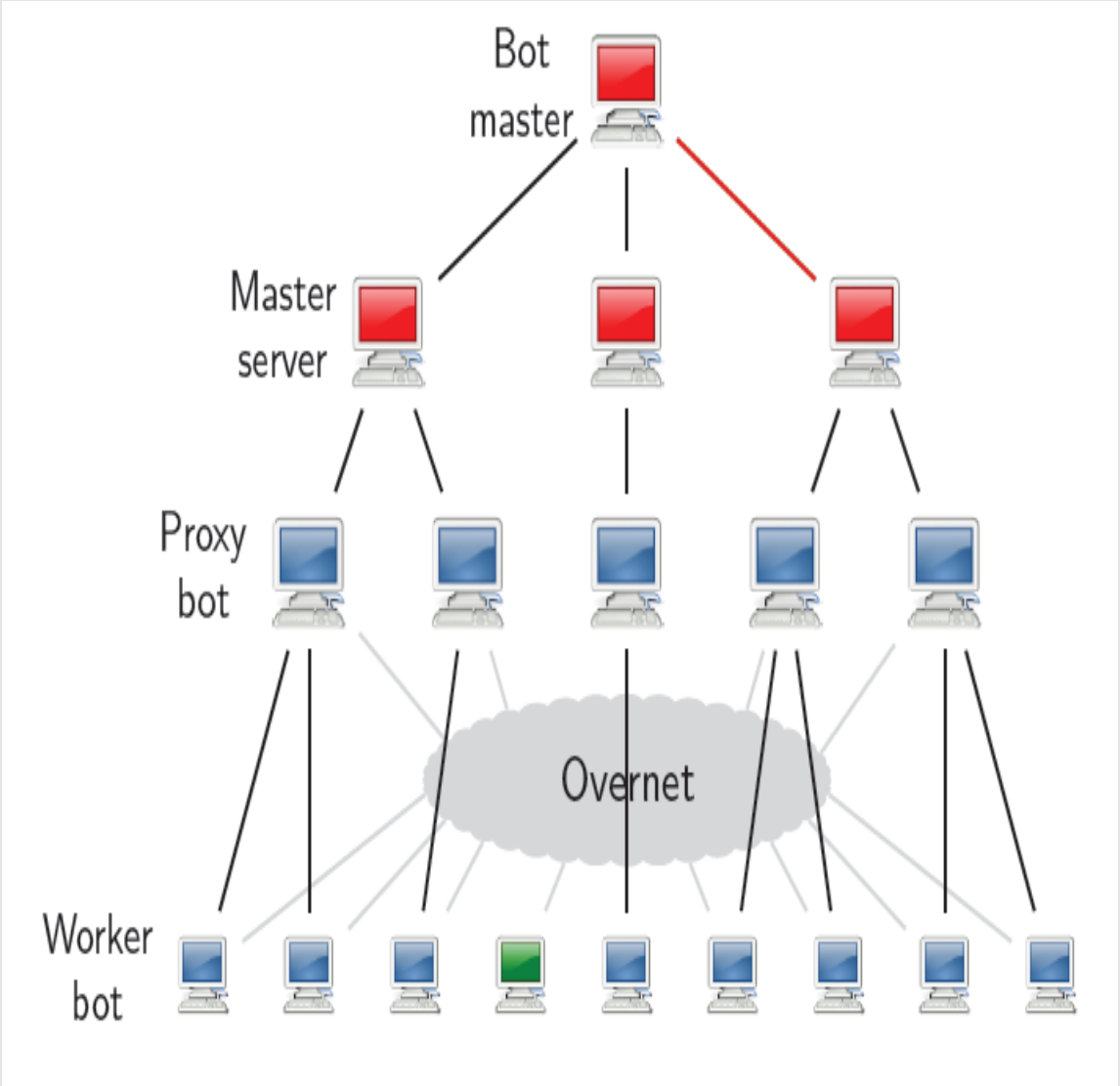
- I worker ricercano le chiavi nella rete P2P per poter localizzare i proxy

Botnet basata su P2P -3



- Una volta localizzati i proxy, ciascun worker si autentica e resta in attesa dei comandi del proxy.

Botnet basata su P2P -4

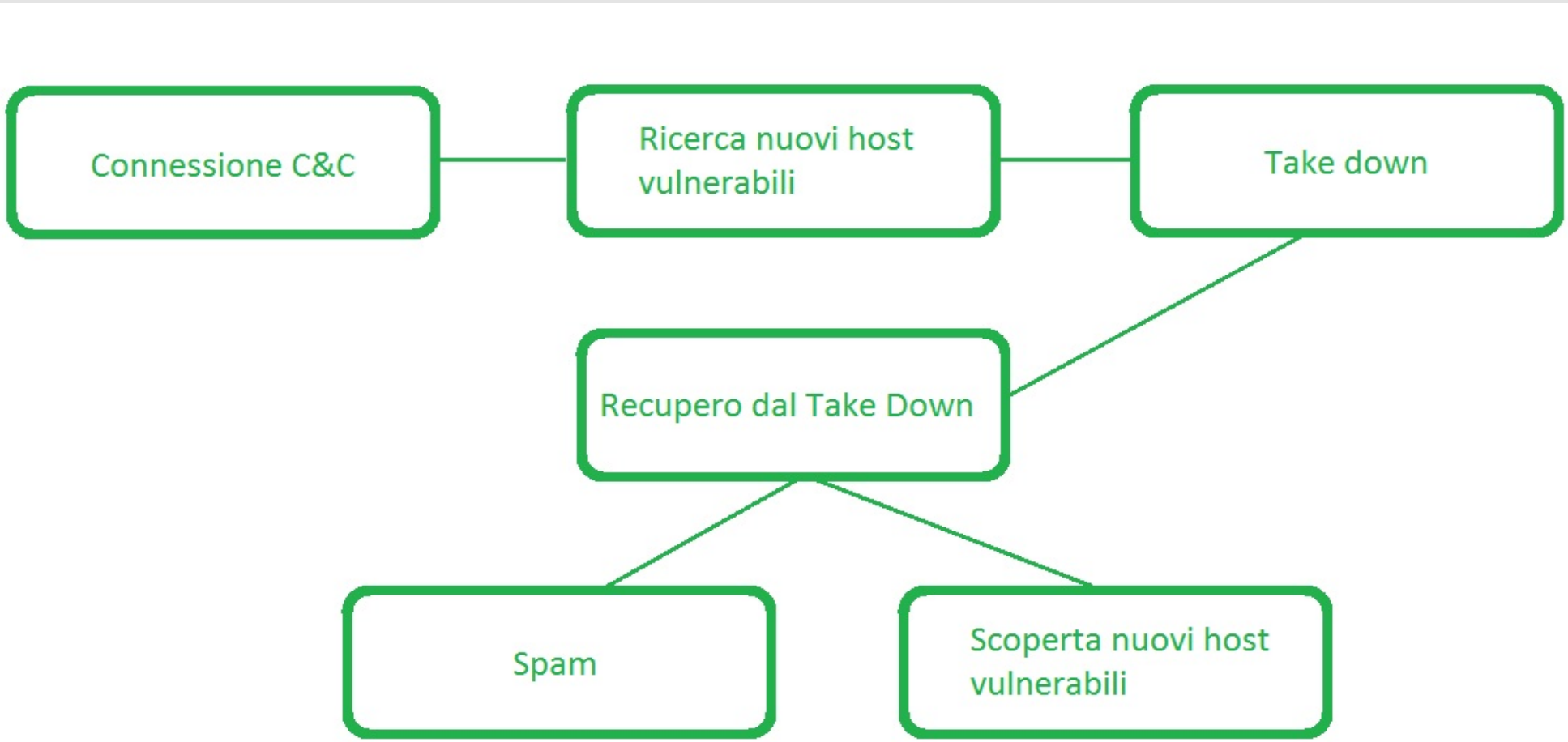


- Il proxy fa da tramite ai comandi del master e alle risposte dei workers.

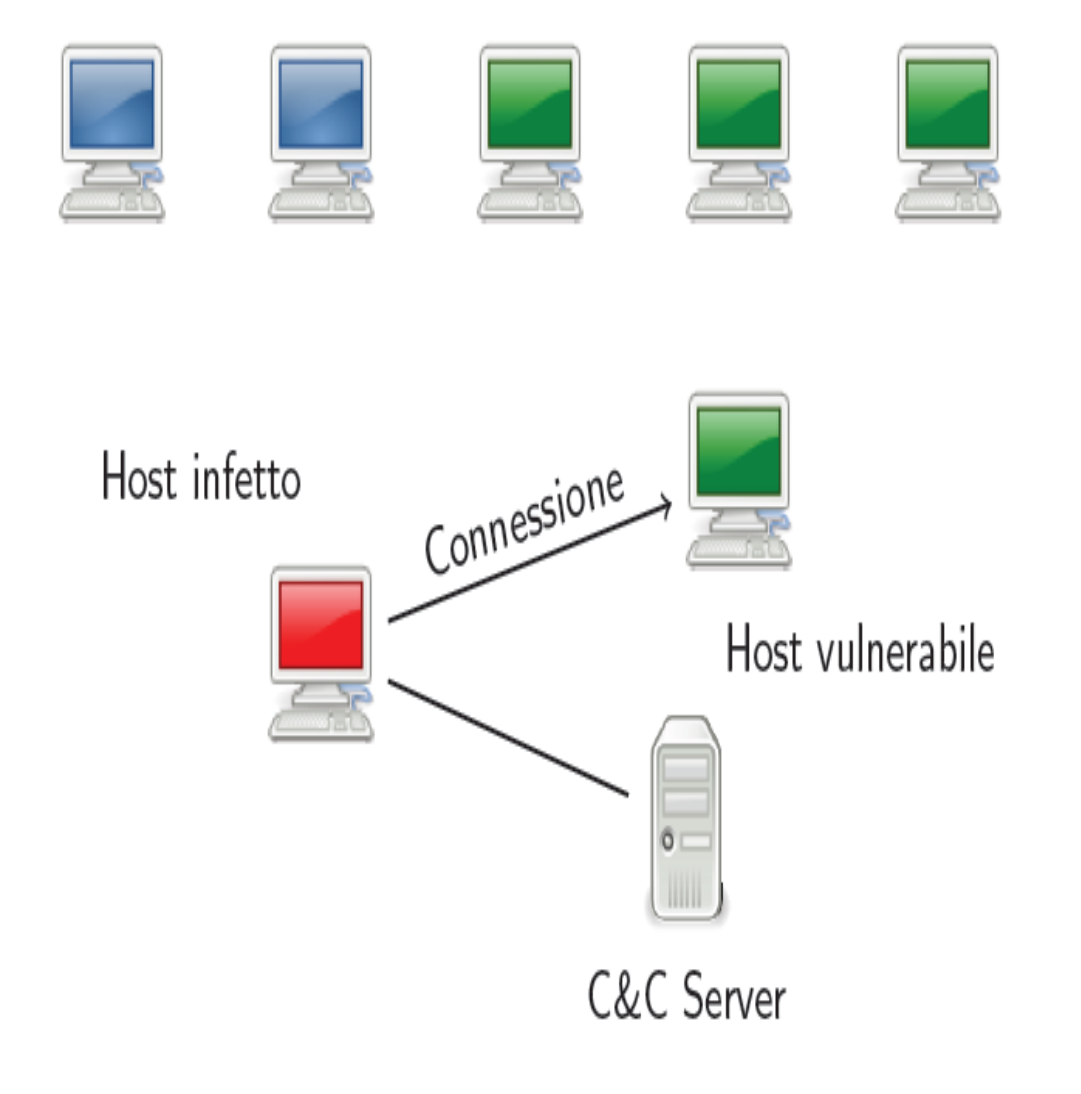
Outline

- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una Botnet
- Infiltrarsi in una Botnet
- Botnet più conosciute
- Difendersi dalle Botnet

Ciclo di vita di un Bot

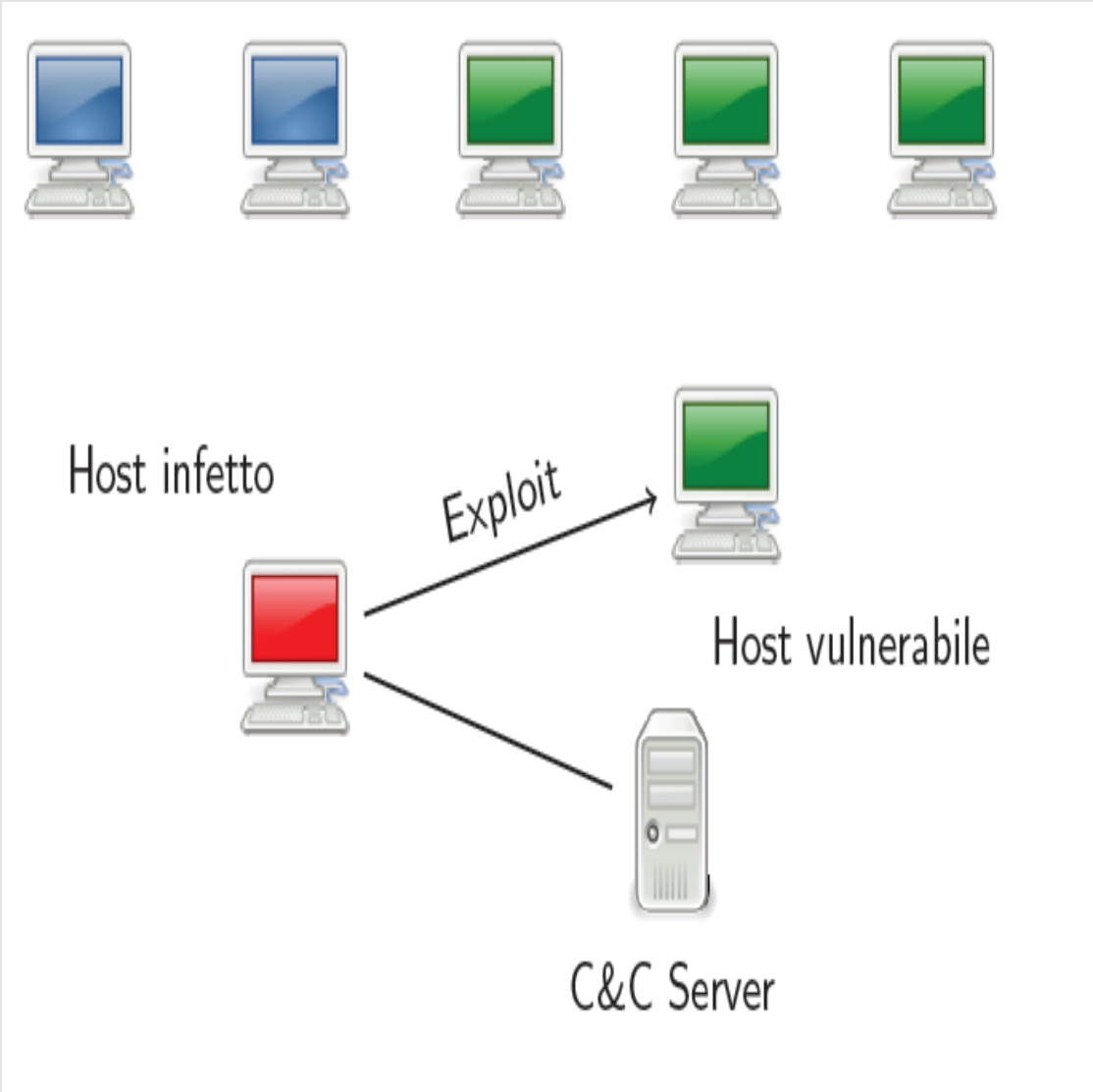


Ciclo di vita di un Bot -2



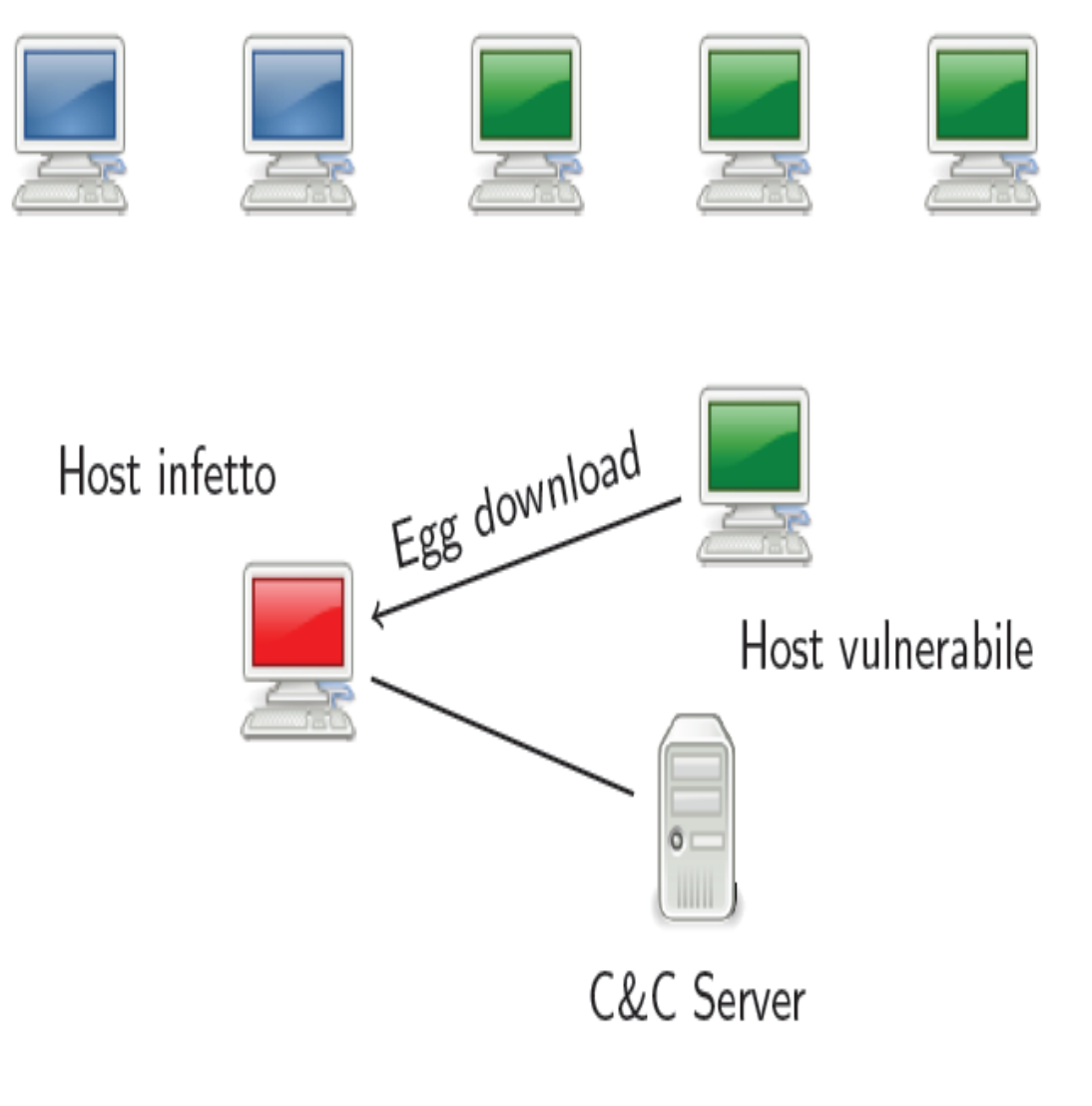
- Il server C&C effettua la ricerca di nuove vittime da infettare tramite un port scan che parte da pc già infetti.

Ciclo di vita di un Bot -3



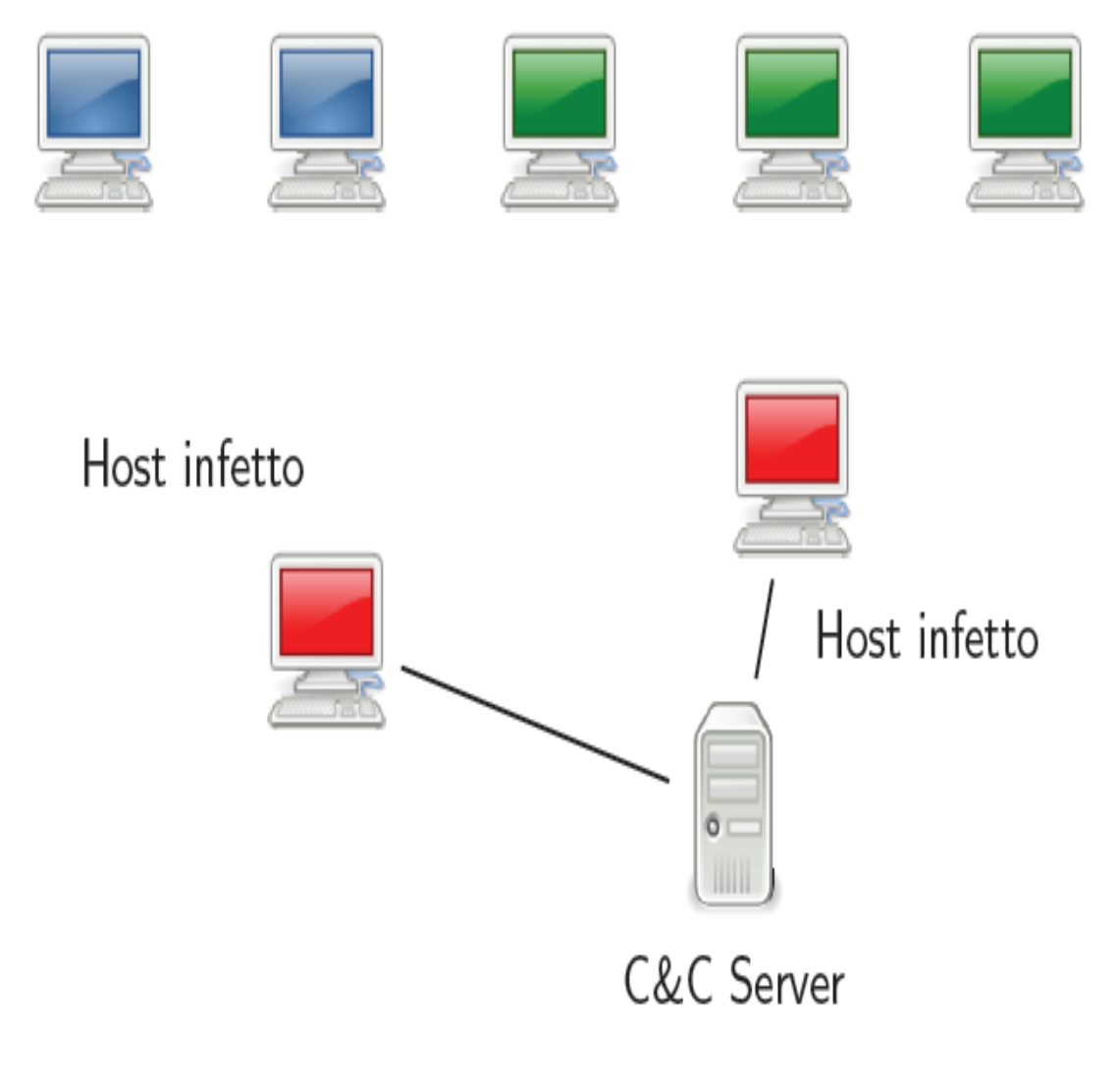
- Tenta di sfruttare una o più vulnerabilità note del sistema attaccato. (Exploit)

Ciclo di vita di un Bot -4



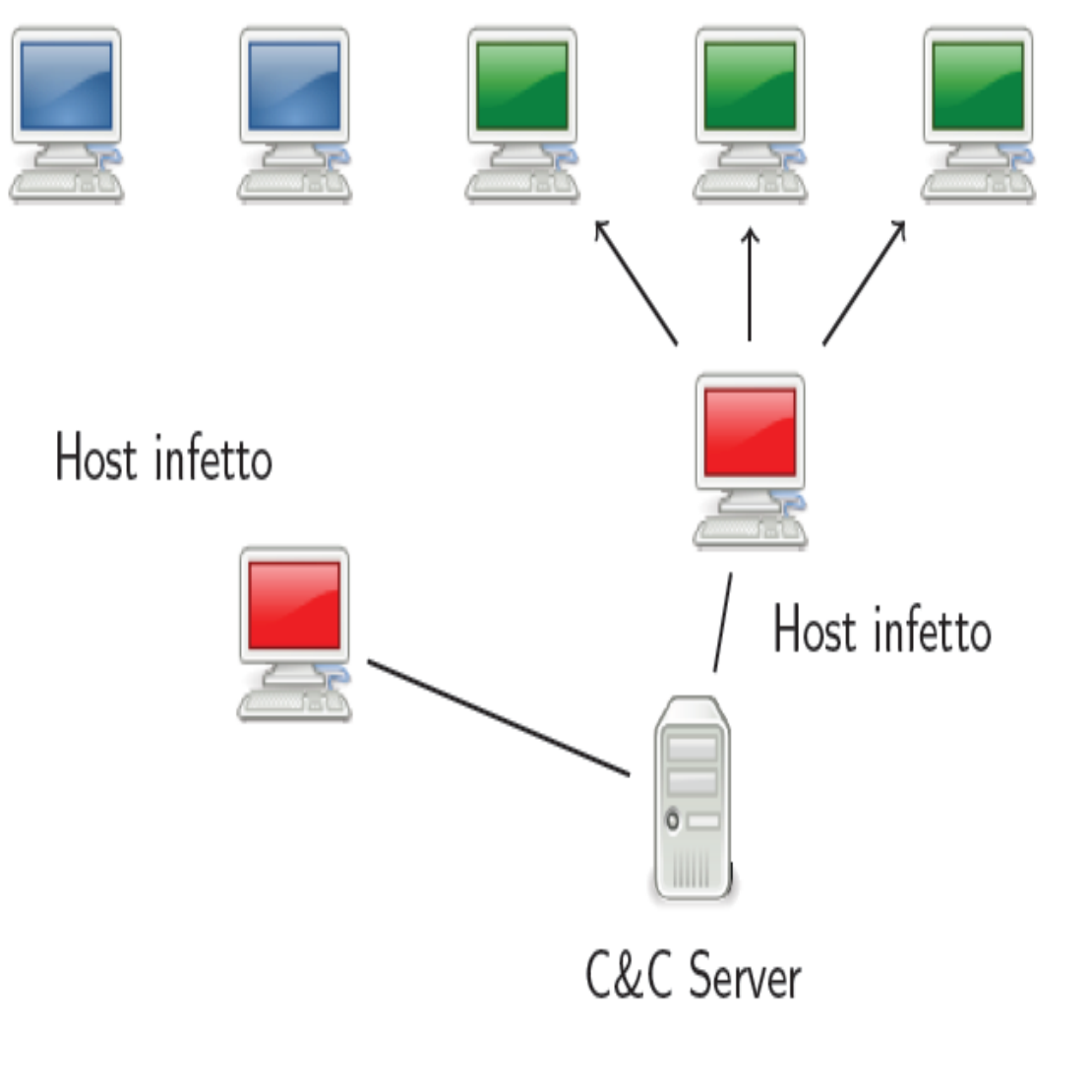
- L'host infetto fa in modo che l'host attaccato gli richieda il download di un egg (codice Bot, rootkit)

Ciclo di vita di un Bot -5



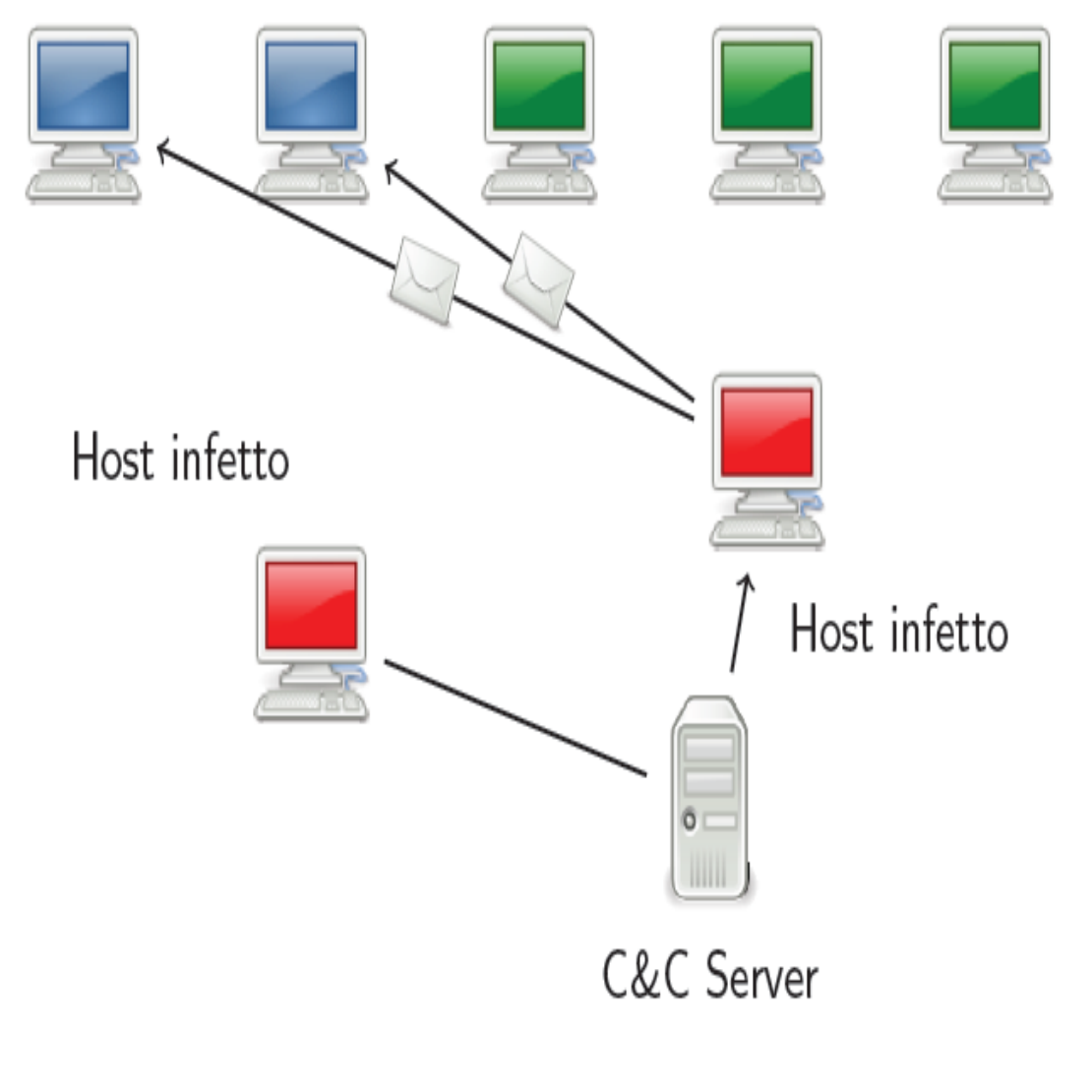
- Dopo essere stato infettato l'host si connette direttamente al server diventando anch'esso uno Zombie.

Ciclo di vita di un Bot -6



- Una volta “conquistato” l'host, il centro di controllo gli può ordinare di cercare altri computer ad esso connesso vulnerabili o di eseguire i comandi impartitigli.

Ciclo di vita di un Bot -6



- Una volta “conquistato” l'host il centro di controllo gli può ordinare di cercare altri computer ad esso connesso vulnerabili o di eseguire i comandi impartitigli.

Outline

- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una Botnet
- Infiltrarsi in una Botnet
- Botnet più famose
- Difendersi dalle Botnet

Attacchi di una Botnet

- DoS
- Adware
- Spyware
- Email spam
- Access number replacement
- Fast Flux

Attacco DoS

- L'attacco più utilizzato, e forse anche il più efficace, tra quelli eseguibili da una Botnet.
- Si fa partire da ciascun Bot della rete una richiesta verso uno stesso sistema o servizio di rete.
- **Effetto:** Il sistema che fornisce il servizio richiesto non risulta più raggiungibile.

Adware & Spyware

- **Adware:** Utilizzato per reclamizzare attività commerciali ad utenti, anche se questi non ne hanno autorizzato l'invio o ne sono a conoscenza.

- **Spyware:** Software utilizzato dal Bot Master per raccogliere informazioni sull'utente e sulle azioni che compie sul suo computer.

Spam & Access number replacement

- **Spam:** sono messaggi email, inoltrati mistificando contatti della rubrica del ricevente; hanno una natura commerciale, fastidiosa e molto spesso maligna.

- **Access number replacement:** si sostituisce il numero di un provider Internet con quello dell'utente che si vuole attaccare. In questo modo egli verrà bombardato dalle chiamate di tutti gli utenti che si servono di quel provider per connettersi ad Internet e sarà costretto a cambiare numero di telefono.

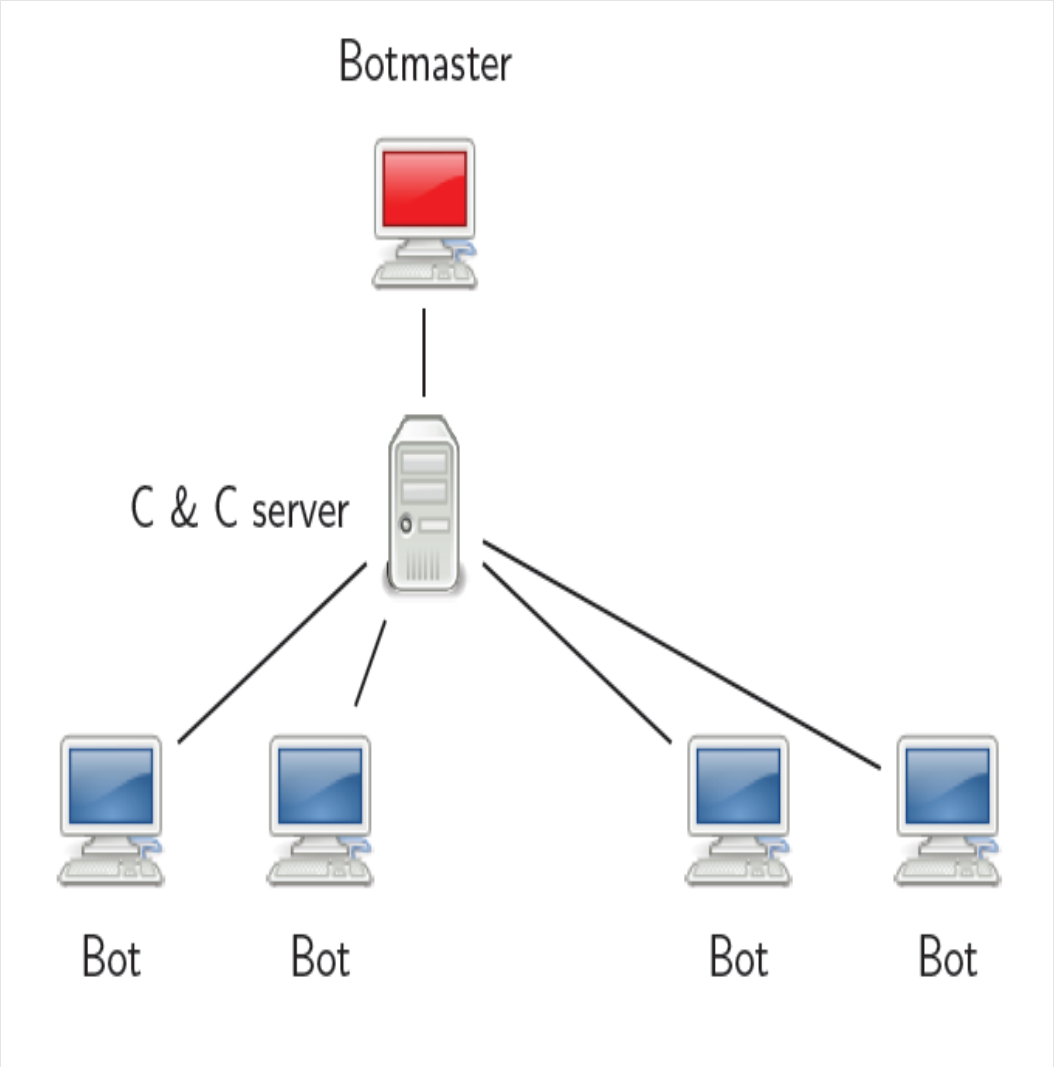
Attacco Fast-Flux

- Questa tecnica è utilizzata soprattutto per nascondere il phishing e i siti che spediscono malware dietro ad una rete di host compromessi e che si comportano come proxy in cambiamento costante.
    - **Single flux:** nodi registrano e de-registrano il proprio indirizzo come parte della lista degli indirizzi DNS per un singolo dominio.
    - **Double flux:** nodi registrano e de-registrano il proprio indirizzo come parte della lista dei record NS per una certa zona.

Outline

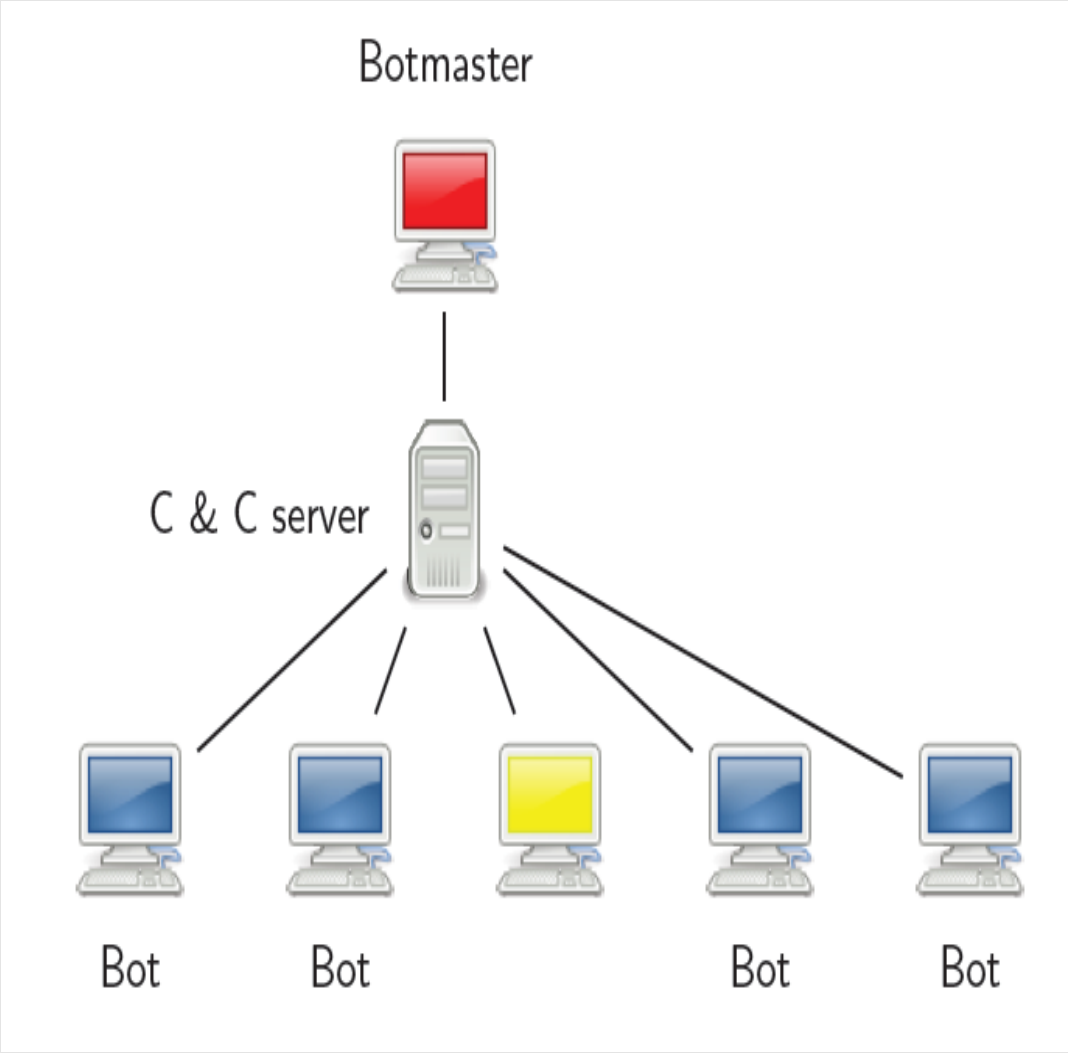
- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una Botnet
- Infiltrarsi in una Botnet
- Botnet più famose
- Difendersi dalle Botnet

Infiltrarsi in una Botnet (IRC)



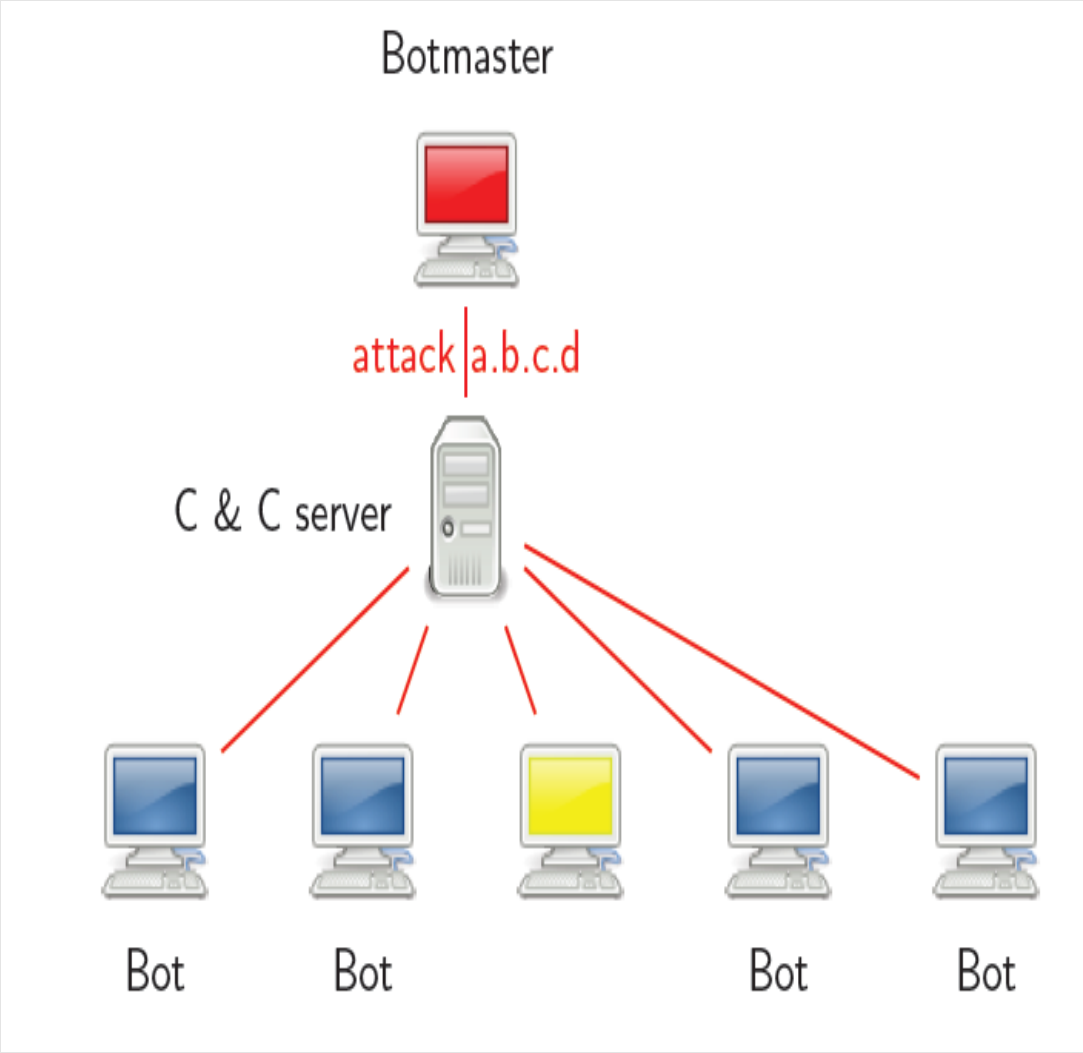
- L'infiltrato si collega al C&C e riesce a vedere tutti gli altri Bot connessi.

Infiltrarsi in una Botnet (IRC)



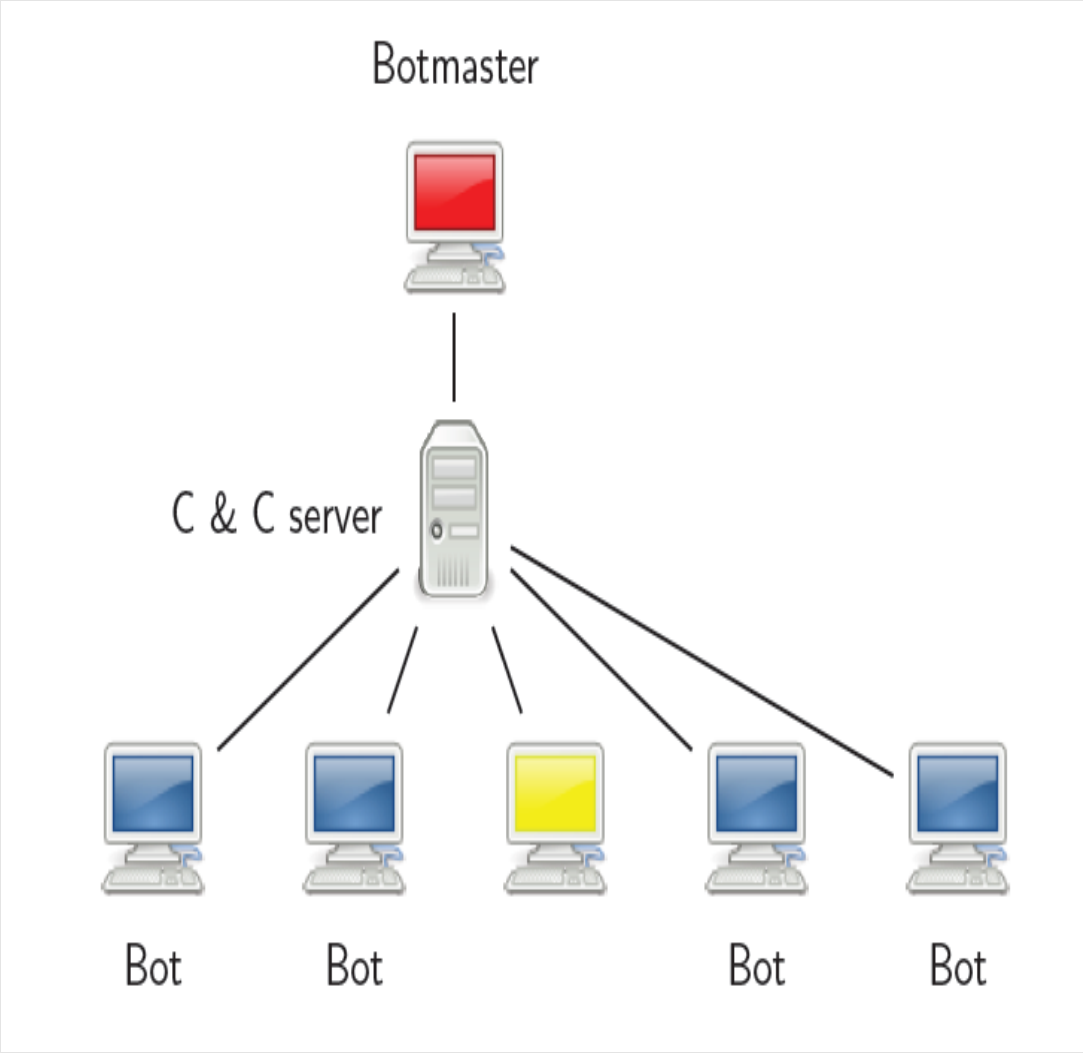
- L'infiltrato si collega al C&C e riesce a vedere tutti gli altri Bot connessi.

Infiltrarsi in una Botnet (IRC)



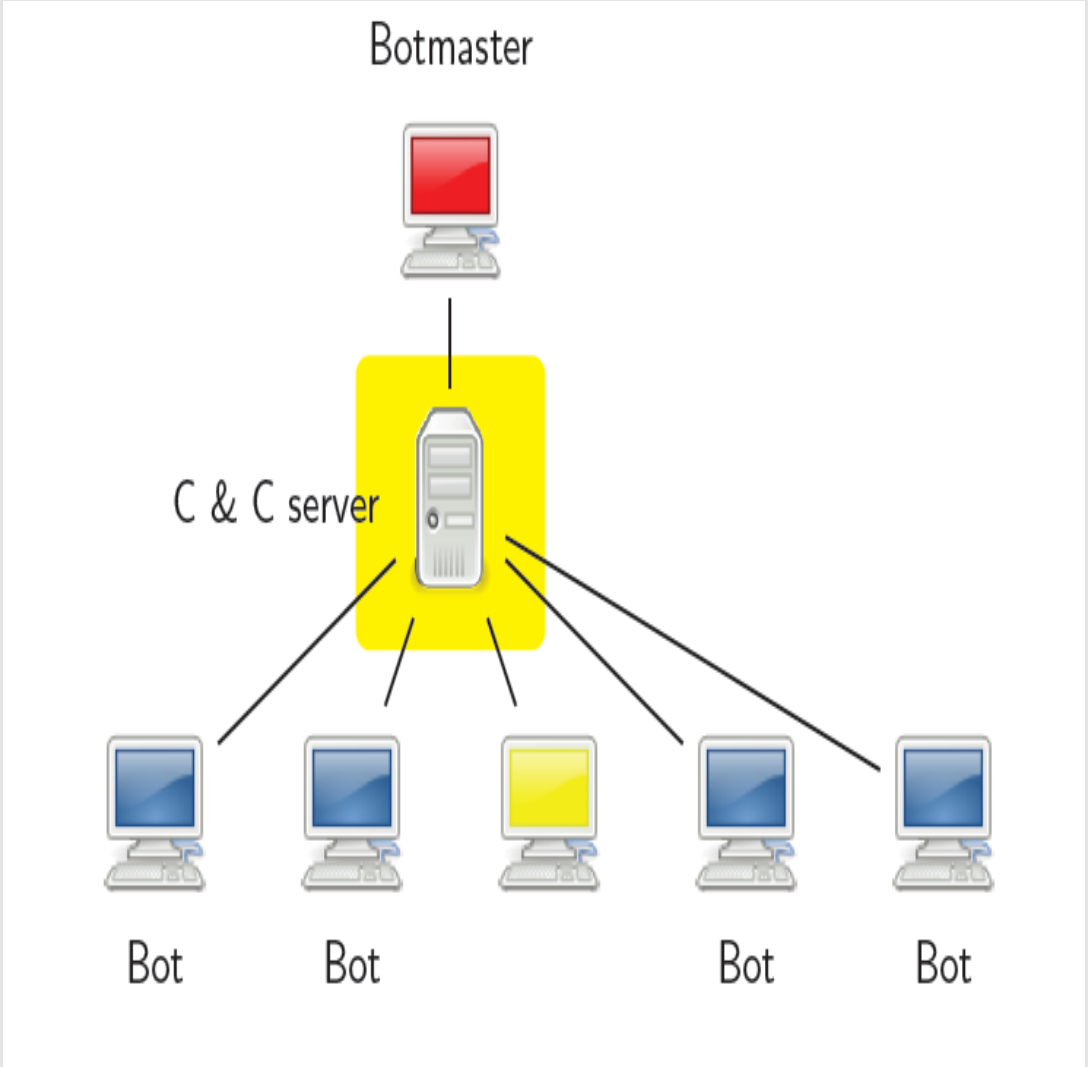
- Anche l'infiltrato riceve i comandi destinati ai Bot.

Infiltrarsi in una Botnet (IRC)



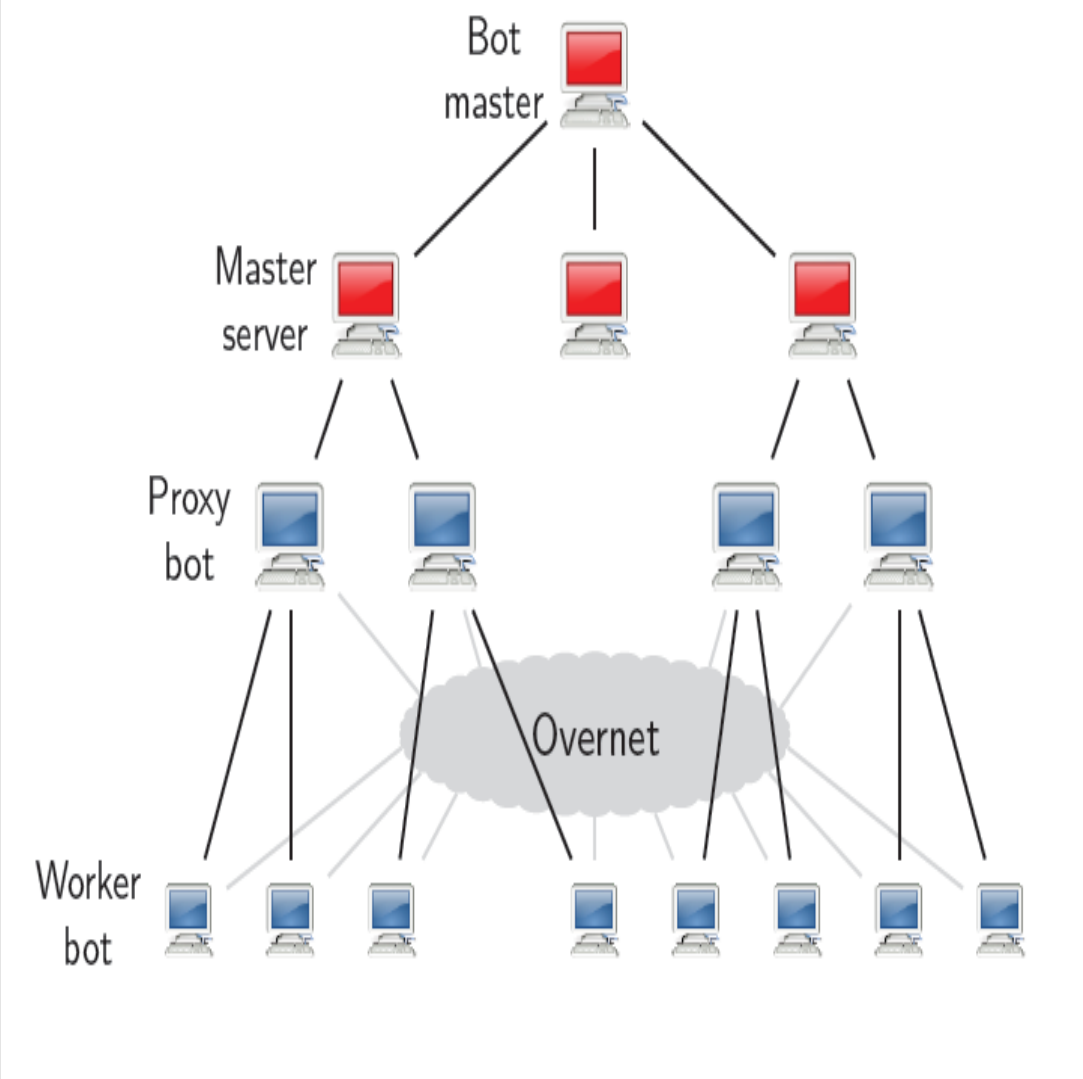
- L'infiltrato può inviare comandi egli stesso ai Bot della rete.

Infiltrarsi in una Botnet (IRC)



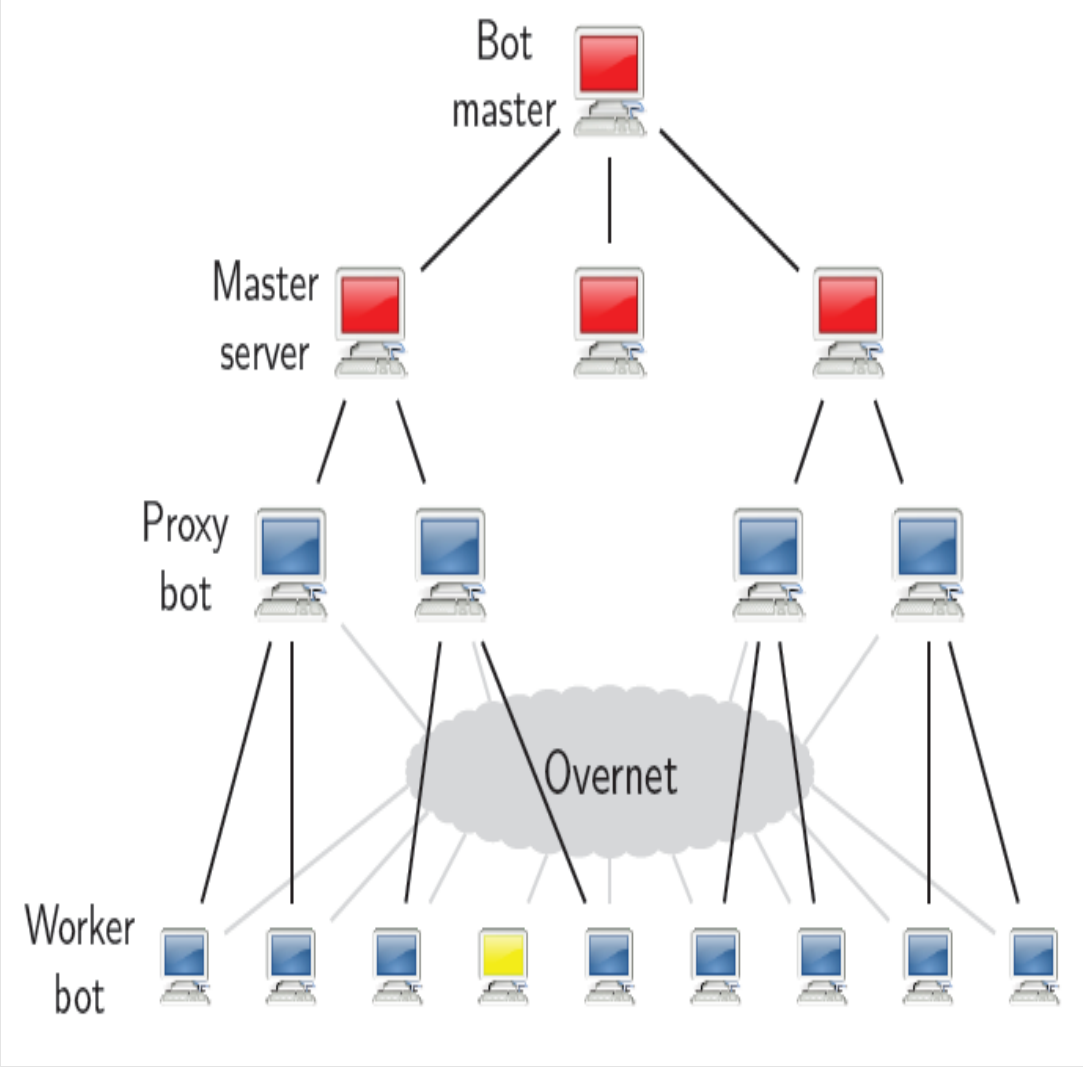
- L'infiltrato può inviare comandi egli stesso ai Bot della rete.

Infiltrarsi in una Botnet (HTTP)



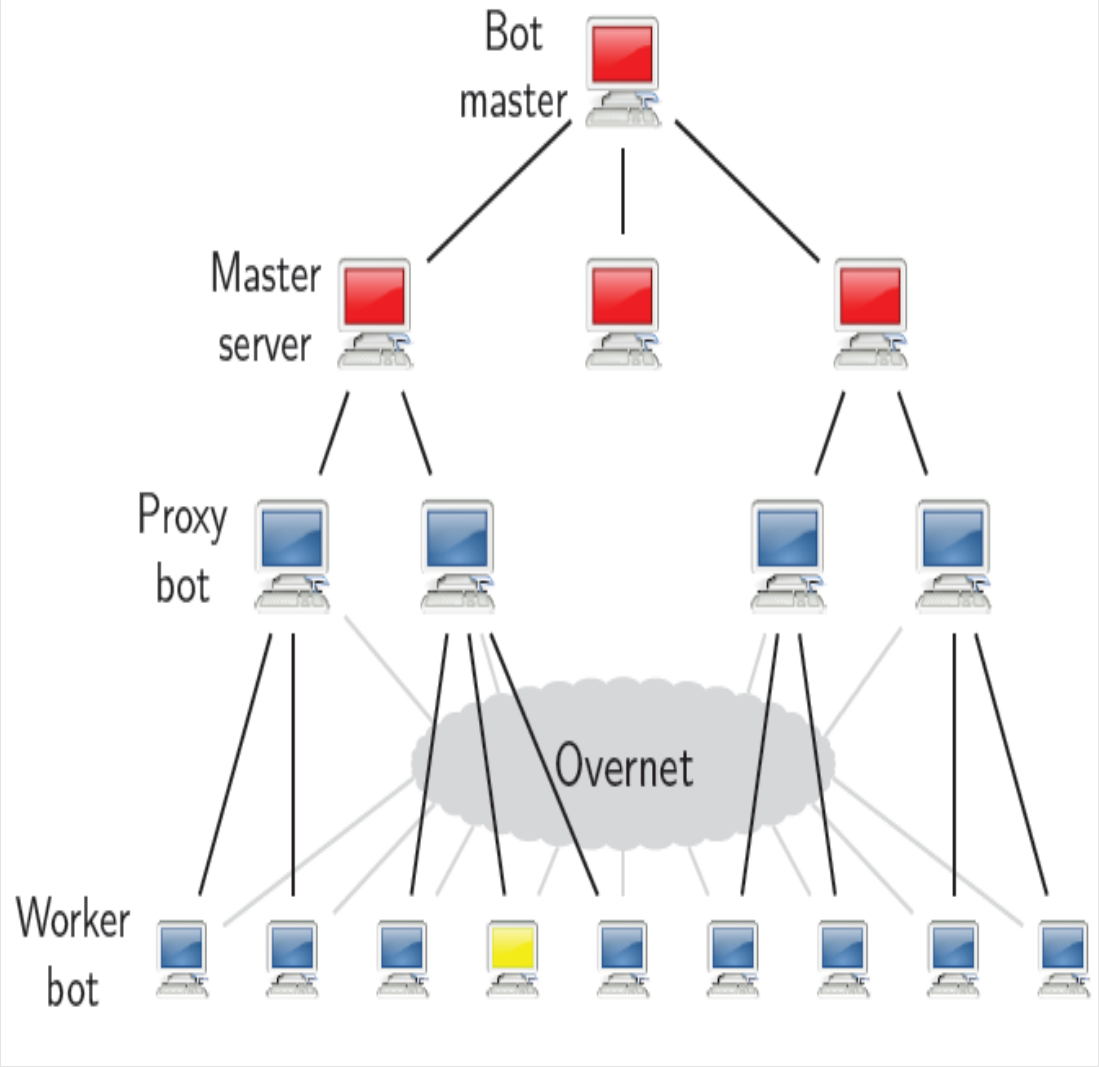
- L'infiltrato si collega al C&C come qualsiasi altro Bot ma non è in grado di vedere gli altri Bot.

Infiltrarsi in una Botnet (HTTP)



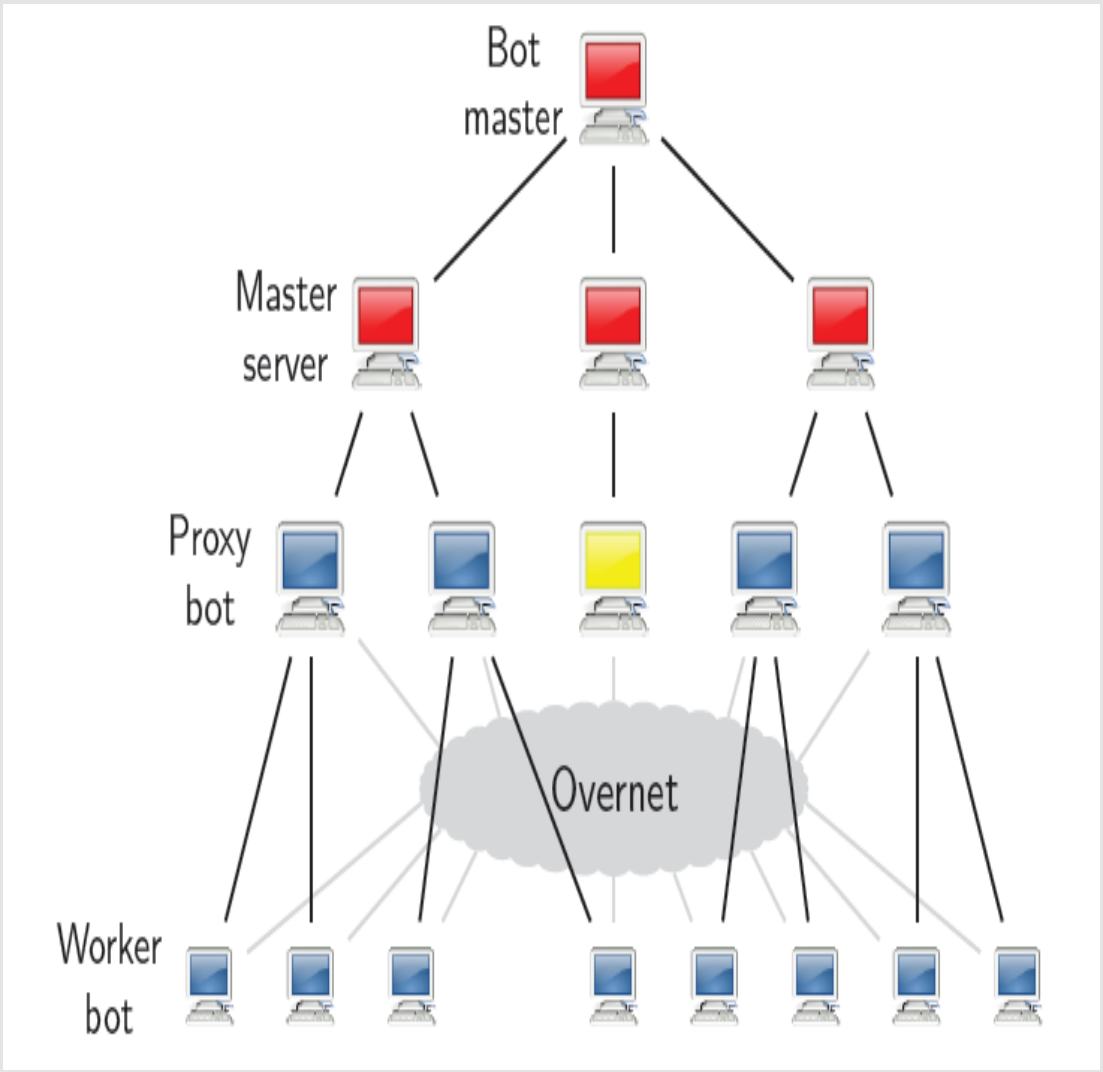
- L'infiltrato riceve comandi dal Botmaster ma non è in grado di mandarne agli host infetti della rete.

Infiltrarsi in una Botnet (HTTP)



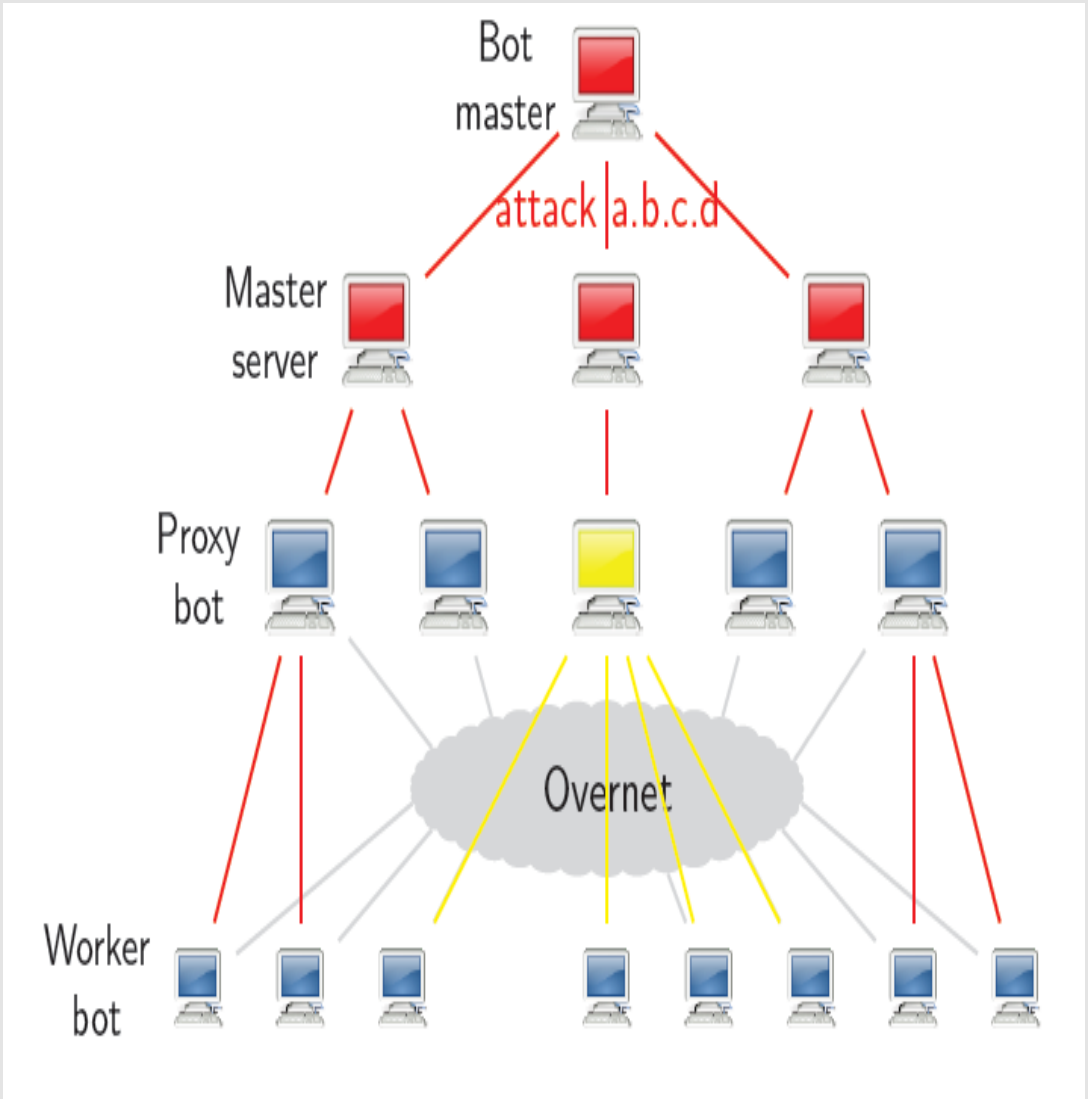
- Se l'infiltrazione dovesse avvenire lato server allora i comandi possono essere mandati anche agli altri Bot.

Infiltrarsi in una Botnet (P2P)



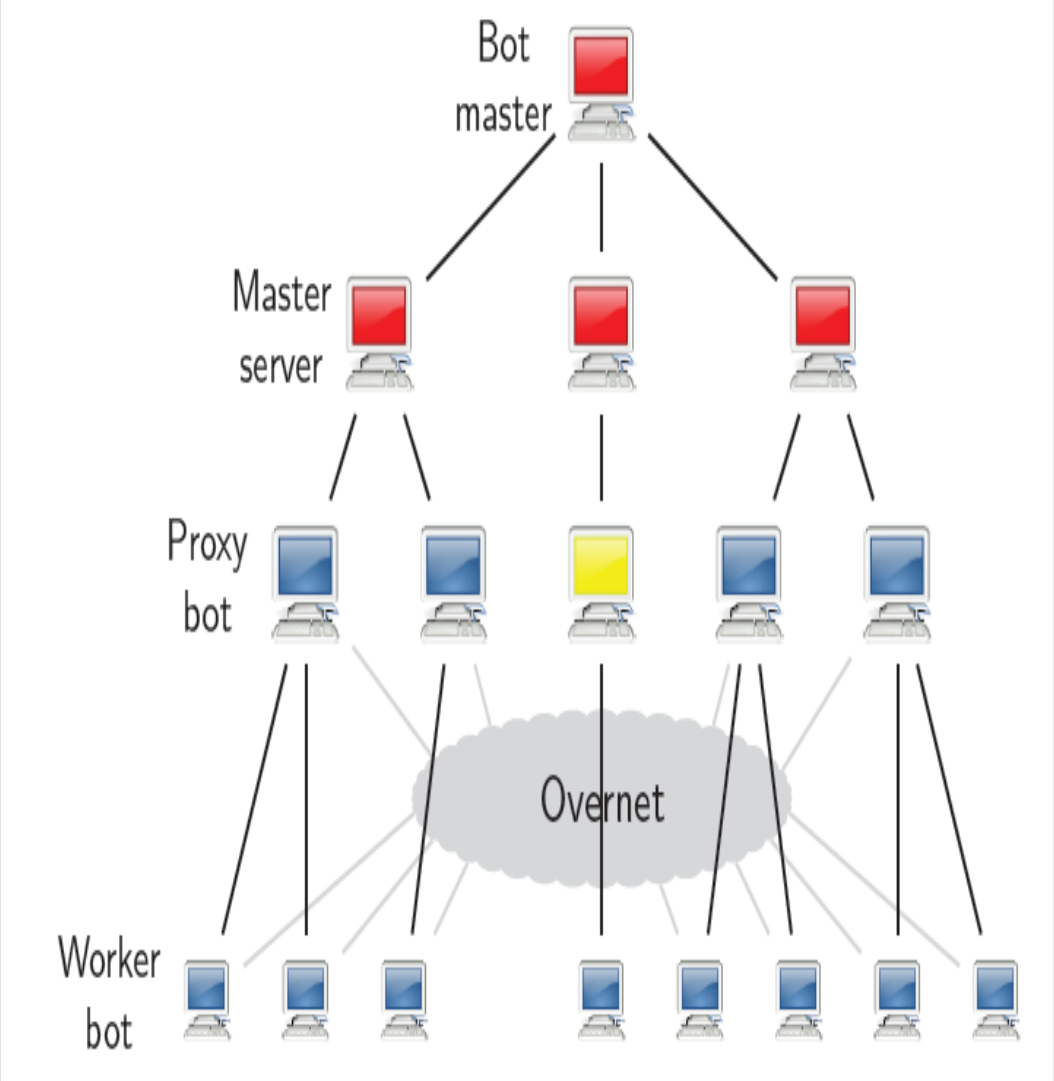
- Il Bot si connette alla rete P2P come se fosse un host infetto per avere le chiavi.

Infiltrarsi in una Botnet (P2P)



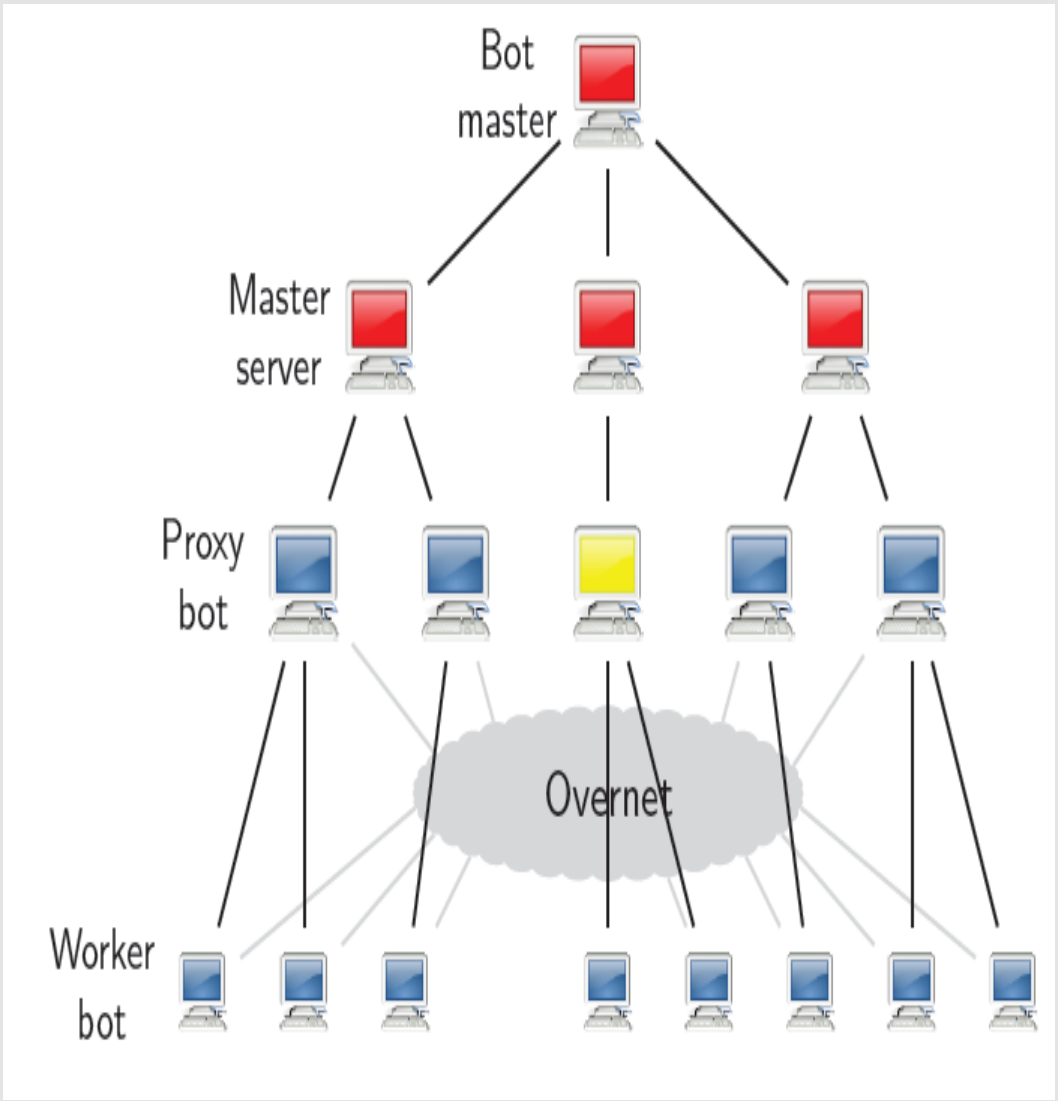
- L'infiltrato si collega al proxy e riesce a vedere i comandi inviati ai Bot.

Infiltrarsi in una Botnet (P2P)



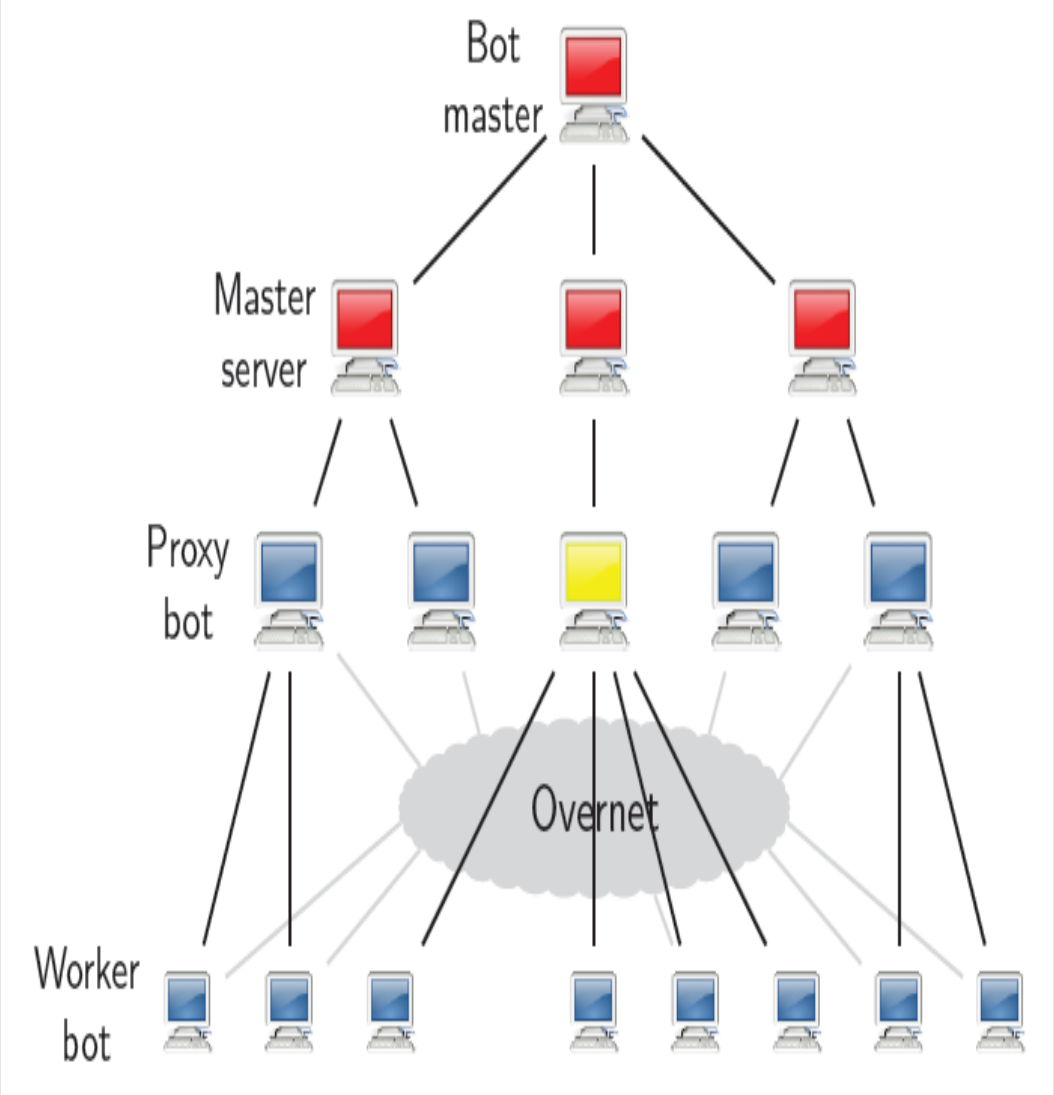
- L'infiltrato potrebbe elevarsi a proxy ed essere quindi capace di
  - Accettare connessioni
  - Enumerare e Identificare Bot ad esso connessi

Infiltrarsi in una Botnet (P2P)



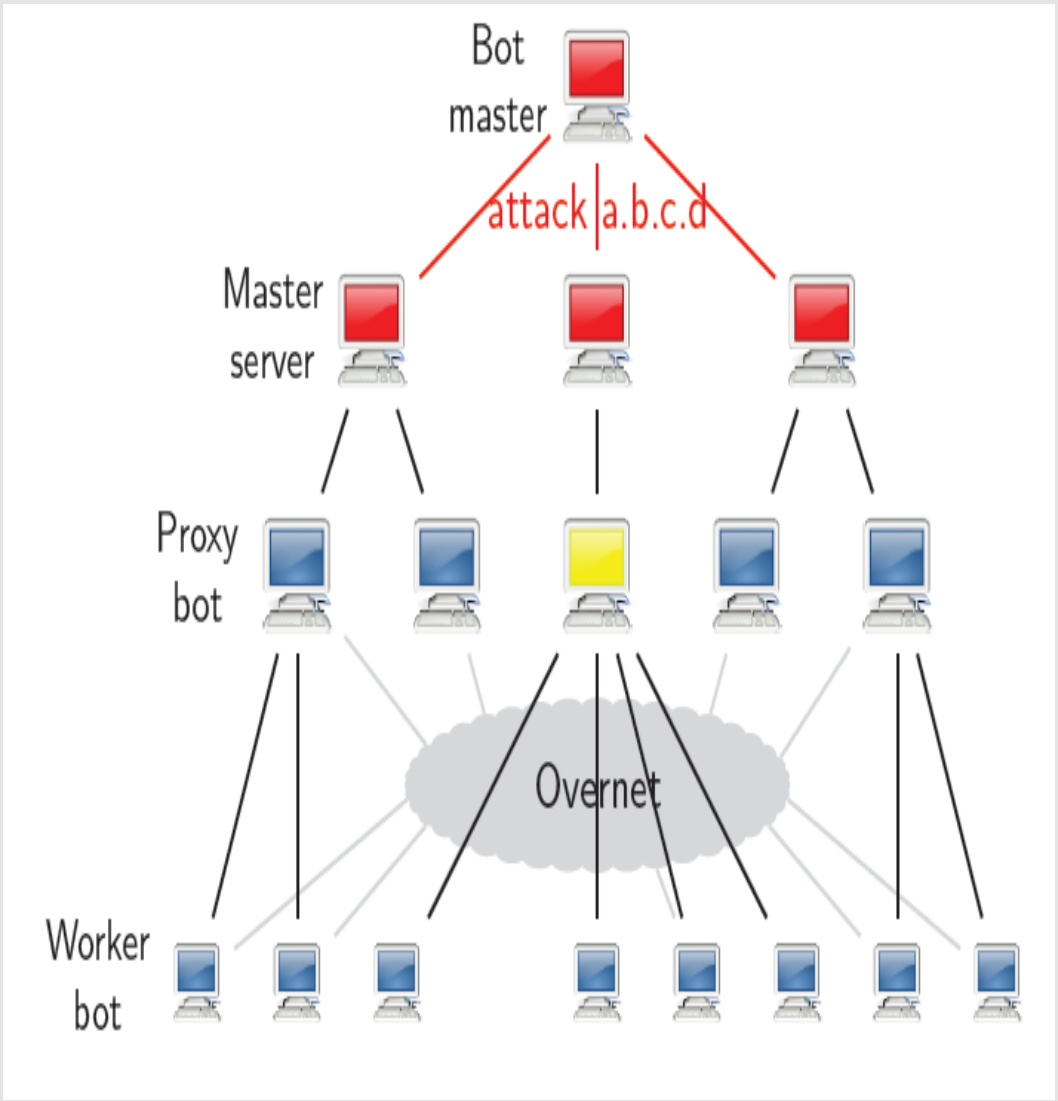
- L'infiltrato potrebbe elevarsi a proxy ed essere quindi capace di
  - Accettare connessioni
  - Enumerare e Identificare Bot ad esso connessi

Infiltrarsi in una Botnet (P2P)



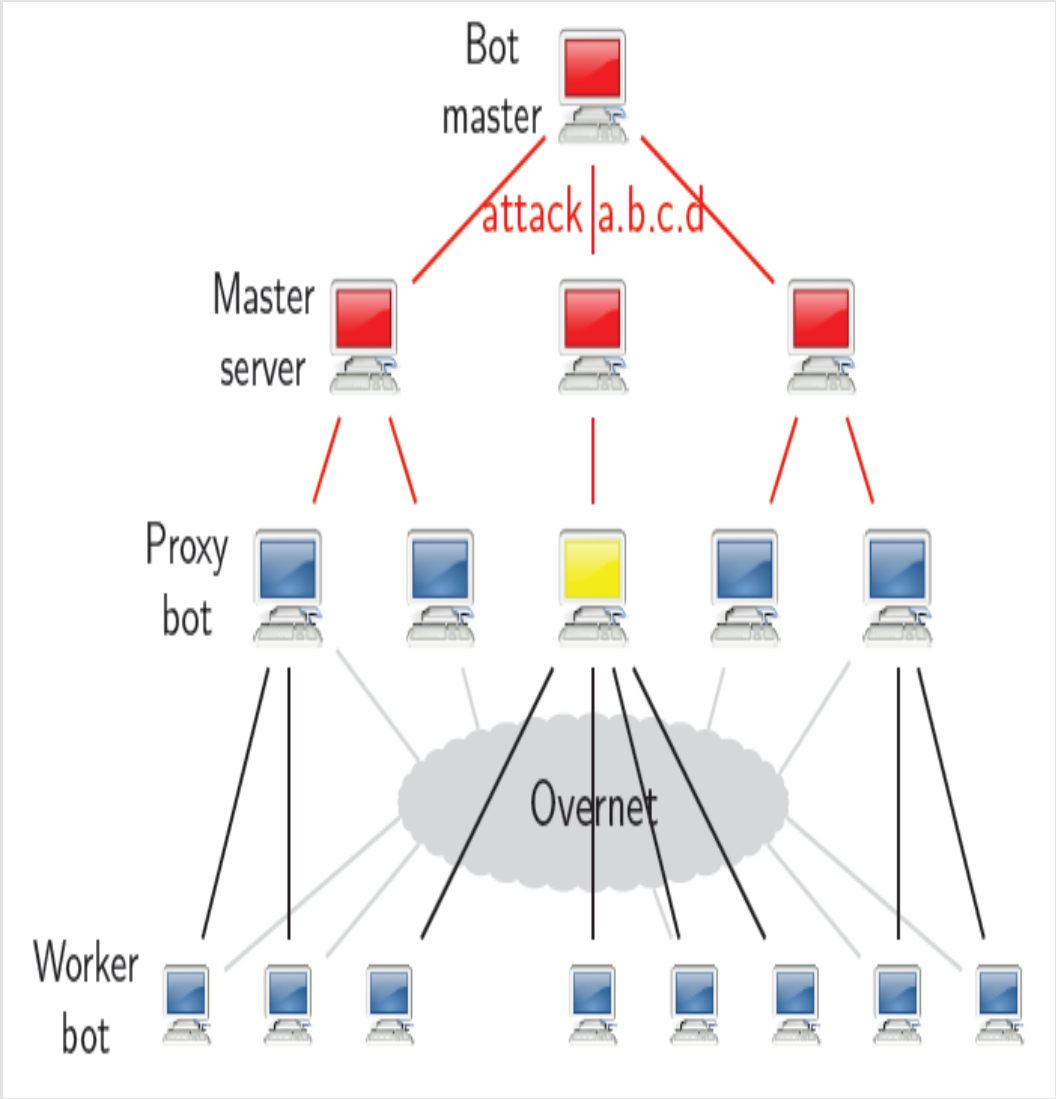
- L'infiltrato potrebbe elevarsi a proxy ed essere quindi capace di
  - Accettare connessioni
  - Enumerare e Identificare Bot ad esso connessi

Infiltrarsi in una Botnet (P2P)



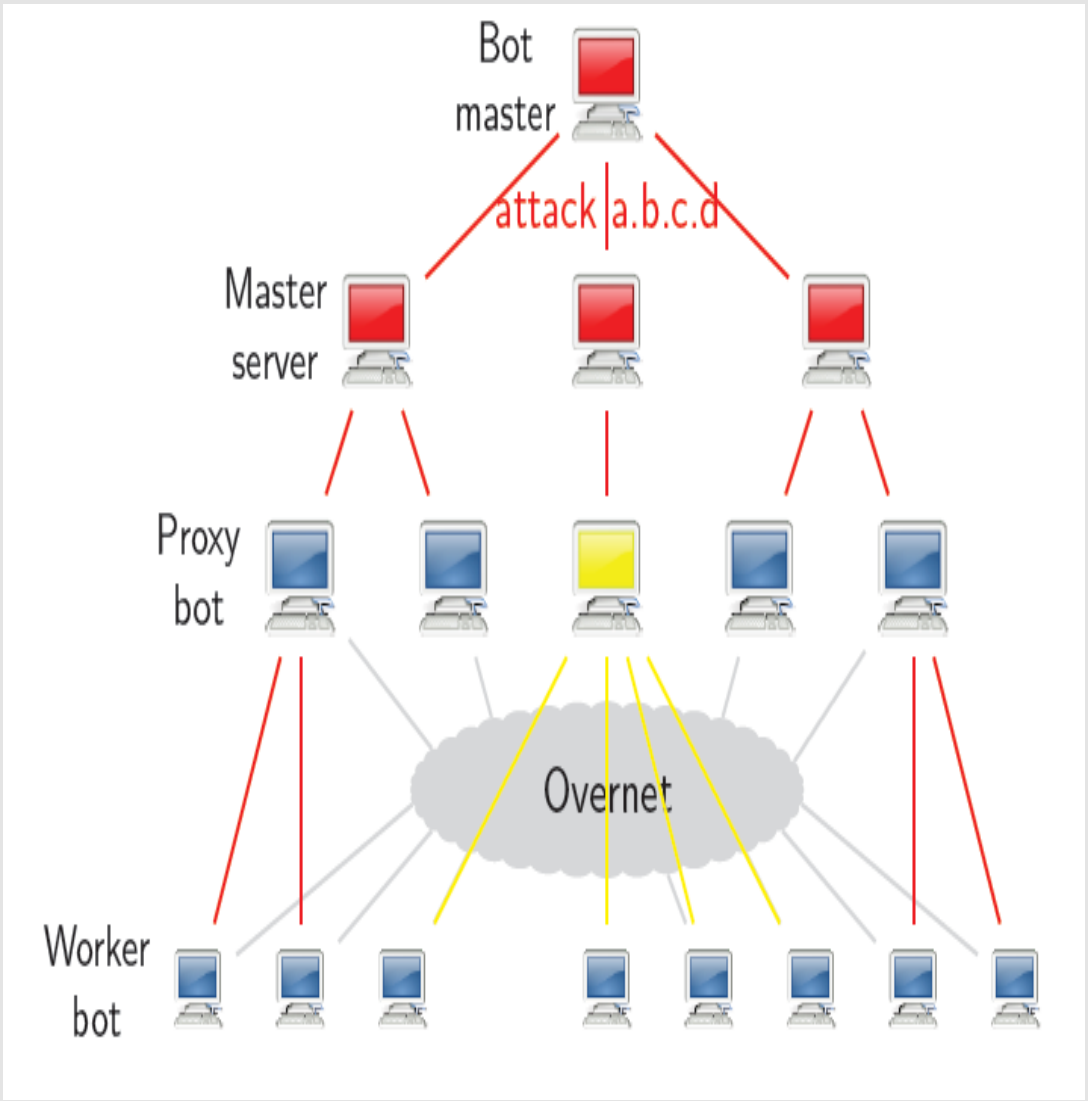
- L'infiltrato potrebbe elevarsi a proxy ed essere quindi capace di
  - Accettare connessioni
  - Enumerare e Identificare Bot ad esso connessi

Infiltrarsi in una Botnet (P2P)



- Il nuovo proxy ha il pieno controllo dei bot ad esso connessi

Infiltrarsi in una Botnet (P2P)



- Il nuovo proxy ha il pieno controllo dei Bot ad esso connessi

Outline

- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una Botnet
- Infiltrarsi in una Botnet
- Botnet più conosciute
- Difendersi dalle Botnet

Botnet più conosciute

Conflicker

Storm

Psib0t

Osx.Iservice

Conflicker

- Conosciuta come Downup, Downadup o Kido è stata identificata per la prima volta nel 2008.
- Bersaglia sistemi Windows tramite exploit MS08-67
- Il worm usa una combinazione di tecniche malware avanzate che sono difficili da contrastare.
- È considerata la più grande infezione da parte di un worm dal 2003.

Conflicker -2

- Questa Botnet ha la particolarità di aggiornarsi e migliorarsi automaticamente. Per questo motivo ne esistono 5 varianti:

VARIANTE	EFFETTO
A	Sfrutta l'exploit dell'aggiornamento MS08-067 ed ha la particolarità di evolversi nelle varianti B, C, D per prolungare l'infezione del sistema.
B	Vengono aggiunte le caratteristiche di phone home, crack della password di rete con conseguente DoS del router a cui si tenta di accedere.
C	Ha la capacità di ricopiarsi in maniera automatica in una DLL a caso. Riesce a cancellare tutti i punti di ripristino esistenti sull'host infettato. Incorpora un thread per la rete P2P e un altro thread che si occupa di scegliere il rendez vous point da un insieme di 50.000 domini.
D	Molto simile alla precedente variante, ma ha la capacità di idetificare e bloccare gli anti malware. Infine si evolve nella variante *E.*
E	Aggiunge alla precedente variante la capacità di correggere MS08-067 in modo da permettere nuovamente l'infezione del pc.

Storm

- La più famosa tra le Botnet
- Creata grazie al trojan Worm Storm inviato come spam.
- È stato stimato che da settembre 2007 questa Botnet abbia compromesso circa 1 milione di PC.
- È stata usata per una miriade di attività criminali.

Storm -2

- 6.000 Bot preposti allo scopo di diffondere il worm.
- Offerta di musica gratuita per attirare le vittime verso siti adibiti all'infezione.
- Codifica ripetuta del Worm.
- Ubicazione dei server remoti protetta con tecnica fast-flux su DNS.
- I Bot entrano a far parte della rete attraverso l’esecuzione di alcuni programmi.

Componenti Storm

Nome File	Compito
Game0.exe	Backdoor/downloader
Game1.exe	SMTP relay
Game2.exe	Email address stealer
Game3.exe	Email virus spreader
Game4.exe	DdoS attack tool
Game5.exe	Updated copy of Storm Worm dropper

PsiB0t

- La maggior parte delle Botnet sfrutta debolezze di Windows, ma anche i sistemi che montano Mac OS e Linux non sono al sicuro.
- Da qualche tempo infatti anche i router basati su Linux corrono il rischio di essere infettati.
- Tale Botnet sfrutta le politiche di sicurezza dell'utente finale. Possiede infatti un DB che comprende 6000 username e 13000 password.

Psib0t -2

- Il worm localizza il router vulnerabile e si connette ad esso tramite telnet.
- Effettua il login come root.
- Scarica un eseguibile tramite *wget.*
- Avvia tale eseguibile che si occupa di:
  - Impedire ulteriori connessioni tramite telnet.
  - Stabilire una connessione con un server IRC.
  - Associare il pc ad un canale IRC per ricevere i comandi.
- Il router compromesso inizia la scansione della rete alla ricerca di altri router da infettare e arruolare nella Botnet.

OSX.Iservice

- Malware diffuso tramite sharing illegale di software sulla rete P2P.
- Tale malware carpisce la password di accesso per assumere poi il controllo dei sistemi attaccati.
- Si sfrutta una copia di iWork'09 o Adobe Photoshop CS4 modificata in modo da installare anche il codice maligno.
- Questo è stato il primo tentativo di creare una Botnet di Mac che sia andato a buon fine.

Outline

- I nuovi attacchi alla rete
- Cos'è una Botnet
- Ciclo di vita di un Bot
- Attacchi di una botnet
- Infiltrarsi in una Botnet
- Botnet più famose
- Difendersi dalle Botnet

Come proteggersi dalle Botnet

- Vi sono diverse contromisure che possono essere attuate per difendersi dalla contaminazione o da un eventuale attacco delle Botnet.
- Le azioni possono avere 3 diferenti scopi:
  - **Prevenzione**: misure che un utente o l'amministratore di un sistema può prendere per proteggere i loro sistemi dalla contaminazione.
  - **Identificazione**: misure che possono essere adottate dall'utente o l'amministratore di sistema per identificare una Botnet malefica.
  - **Risposta**: azioni che un utente o l'amministratore di un sistema potrebbe intraprendere in risposta alle infezioni delle Botnet.

Utente – Prevenzione

- Prendere coscienza dell'importanza della sicurezza e della privacy su Internet.
- Seguire le raccomandazioni circa un uso sicuro del S.O.
- Mantenere il S.O. sempre aggiornato e con le ultime patch di sicurezza installate.
- Praticare gestione sicura di mail, IM, e browser.
- Usare e aggiornare costantemente l'antivirus.
- Tenere il Firewall sempre attivo sull'host connesso alla rete.

Utente - Identificazione

- Notare una quantità insolitamente alta di traffico sulla porta 6667.
- Verificare un eccessivo ritardo nelle risposte da parte della rete.
- Ricevere grandi volumi di traffico su porte insolite.
- Identificare dei tipi di Bot conosciuti dall’antivirus.
- Utilizzare risorse online che ispezionino il sistema.

Utente - Risposta

- Disconnettere ogni macchina compromessa da Internet e soprattutto dalla rete locale.
- Aggiornare l’antivirus e installare le patch del sistema operativo.
- Utilizzare tool anti trojan.
- Bloccare tutte le carte i cui dati bancari erano immagazzinati nell’ host compromesso.
- Cambiare tutte le password dell’host attaccato.

Amministratore

- Prevenzione: In aggiunta a tutte le precauzioni che l'utente deve prendere, l'amministratore di un sistema deve anche mantenersi aggiornato sulle ultime vulnerabilità tramite risorse web come *cert.org* o *sans.org*.
- Identificazione: L'amministratore e l'utente devono rivolgere la propria attenzione agli stessi aspetti.
- Risposta: L'amministratore e l'utente dovranno intraprendere le stesse azioni una volta che il sistema sia stato contaminato.

Grazie per la cortese attenzione