Corso di Sicurezza su Reti 2

Le Botnet

Docente: Alfredo de Santis **Studente: Gabriele di Chiara**

Sommario

1. Introduzione

Data la crescente popolarità della rete e più in particolare dell'utilizzo dei siti di e-commerce è cresciuto anche il numero di attacchi che questi sistemi sono costretti a subire da parte dei malintenzionati. Già a partire dai primi anni '80 si è avuto un assaggio di quanto siano pericolosi tali attacchi, infatti è proprio in quegli anni che cominciano a venir fuori i primi hacker. Il loro obiettivo erano i sistemi informatici e telefonici e venivano portati sia per imparare e sfruttare le debolezze dei vari sistemi presenti sulla rete sia per risparmiare sui costi di connessione e delle chiamate utilizzando tali sistemi come ponte o sfruttandone la connessione ad Internet. Col passare degli anni , poi, il numero di hacker è andato sempre più aumentando e l'appartenenza a tale categoria era quasi diventato una moda per gli smanettoni dell'epoca. Con il passare del tempo tali hacker hanno migliorato le loro tecniche di attacco e hanno sempre più frequentemente rinnovato i loro obiettivi, scegliendone sempre di più arditi e difficilmente raggiungibili. Dato il sensibile incremento del numero di hacker sulla rete, è stata una conseguenza naturale il fatto che alcuni di loro si siano riuniti per formare, quelle che allora vennero denominate, *hacker gang* il cui scopo era quello di prendere il controllo dei maggiori sistemi informatici e delle più grandi aziende di telefonia. Nel '95 però il numero di hacker aumentò vertiginosamente e questo sopratutto grazie alla notorietà raggiunta da un mezzo di comunicazione che, a partire da quel momento, avrebbe cambiato per sempre il nostro modo di vivere: Internet. Dato che questo è uno strumento largamente esteso ed è inoltre utilizzato da una varietà di categorie di utenti ampia ed eterogenea, viene molto spesso utilizzato anche per il commercio elettronico e ciò ha portato alla trasformazione dell'hacking in cyber crime. Inoltre solo dal 2001 si è evidenziata importanza della sicurezza dei sistemi informatici e quindi la ricerca accademica ha incominciato a investire una maggiore quantità di sforzo in tale campo. Questo ha scatenato l'avvicinamento dei criminali al mondo degli hacker e quindi all'utilizzo della rete come mezzo per raccogliere denaro tramite le truffe agli utenti più inesperti e sprovveduti. Di seguito è rappresentata una tabella riassuntiva delle attività illegali e dei relativi guadagni ottenuti attraverso i diversi tipi di attacchi;

	Stima	Fonte
Credenziali di conto bancario	$10–$100	Symantec (2008) [19]
Carta di credito	$0.40–$20	Symantec (2008) [19]
Dati per furto di identità (nominativo, SSN, data compleanno, ecc.)	$1–$15	Symantec (2008) [19]
Asta di credenziali di conto	$1–$8	Symantec (2008) [19]

Tabella 1: *Prezzo unitario per la commercializzazione nell'economia sommersa[16]*

	Stima	Fonte
Computer facenti parti di *botte*	5 milioni	Symantec (2008)[19]
Computer infetti con software maligno per furto di identità	10 milioni	Panda Security (2009)[20]
False pagine web usate per il *phishing*	116.000	Moore and Clayton(2009)[21]
Siti web che infettano i visitatori per mezzo di software maligno (*malware*)	3 milioni	Provos et al. (2008)[22]

Tabella 2: *Numero di computer e siti web compromessi[16]*

	Stima	Fonte
Frodi online di banche del Regno Unito (6/2007–5/2008)	£36.5 milioni	APACS (2008)[23]
Perdite dirette dovute a furto di identità negli U.S.A. (2006)	$2.8 miliardi	Gartner (2006)[24]
Danni in Europa causati dal malware (2006)	€9.3 miliardi	Computer Economics (2007)[25]

Tabella 3: *Perdite annue[16]*

Una conseguenza di questo nuovo quadro “industriale” è che mentre il software antivirus in precedenza riusciva ad intercettare la maggior parte del *malware* adesso esso riesce a bloccarne solo una minima parte. I computer infetti sono in grado, inoltre, di registrare i tasti premuti dai loro utilizzatori quando digitano le credenziali per l’*electronic banking*; essi possono anche essere utilizzati per realizzare reti di computer infetti, le *Botnet.* Successivamente verrà data, relativamente a questo tipo di minaccia, una definizione. Successivamente verrà data, relativamente a questo tipo di minaccia, una definizione e una descrizione dettagliata dei componenti che ne fanno parte e soprattutto dei mezzi di comunicazione che verranno utilizzati da questa rete per diffondere la minaccia, in particolare si prenderanno in considerazione il canale IRC, quello http ed infine quello del p2p. Verrà poi presentata una panoramica abbastanza approfondita sulle varie tipologie di worm attraverso cui la minaccia delle Botnet si può espandere.

Nel capitolo 2 verrà anche presentato uno schema di funzionamento della Botnet e un possibile problema che si potrebbe verificare in una rete del genere.

Nel terzo capitolo verranno elencati e descritti in maniera approfondita tutti i tipi di attacchi apportabili attraverso questo tipo di rete, tra i quali il più importate è sicuramente quello di DDoS. Verranno poi presentate dei metodi per infiltrarsi in una Botnet e successivamente una breve panoramica delle Botnet più famose.

Infine nell’ultimo capitolo verranno proposti vari accorgimenti e consigli per potersi difendere dalla contaminazione di questa minaccia. Tale mezzo viene sfruttato perché si riescono a raccogliere soldi velocemente ed in grosse quantità grazie al suo ampio bacino d’utenza. Come si può vedere, sin dalla sua nascita quindi, la sicurezza della rete è sempre stata uno dei principali problemi a cui bisognava prestare massima attenzione; bisogna infatti, prendere in considerazione tutti i possibili tipi di attacco che un pirata informatico può effettuare nei confronti della nostra rete e adottare le giuste misure di sicurezza, senza sottovalutare nessun particolare seppur minimo. Ovviamente oggi le metodologie di attacco si sono evolute ed il loro scopo è solitamente

quello di tentare di frodare l'utente onde sottrargli informazioni personali molto riservate. Possiamo quindi dire che gli hacker riescono ad apportare attacchi che possono essere sia ad alto che a basso livello. Si è potuto notare che col passare degli anni ciò che è cambiato è stato proprio il rapporto tra tecnologia e criminalità che è diventato sempre più stretto e c'è sempre stata una sorta di competizione tra quelli che vogliono renderla un mezzo di comunicazione sicuro e quelli che ne sfruttano le debolezze per scopi maligni. Tra gli attacchi più comuni che possono essere portati alla rete ci sono:

1. Hacking di applicazioni web: visto l'affermarsi della rete come mezzo di comunicazione, molte aziende hanno deciso di rivolgere il loro interesse verso Internet e lo hanno fatto grazie allo sviluppo di applicazioni web che consentissero all'utente di effettuare acquisti su Internet. Queste applicazioni web non sono ovviamente sicure al 100% e gli hacker cercano in vari modi di rubare dati personali e numero di carte di credito infiltrandosi in queste applicazioni. Alcuni dei metodi più comuni sono:
   - Cookie Poisoning
   - Hidden field
   - Parameter Tampering
   - SQL Injection
   - XSS

2. Phishing: Tale attacco viene usato per carpire informazioni sensibili o personali dell'utente. Di solito questo avviene tramite l'invio di una mail contenente un link che l'utente dovrà seguire per regolarizzare una presunta situazione di anormalità. Il sito a cui l'utente verrà indirizzato è una copia fittizia di un sito molto conosciuto e riporterà alcuni dati che l'utente dovrà correggere e inviare al sito. Una volta inviati questi dati al server, questo li memorizzerà e quindi il phisher li potrà usare per fare acquisti su Internet o magari anche sfruttare tale terminale come ponte per i suoi attacchi ad altri sistemi.

3. Vishing: Non è altro che il phishing fatto sul protocollo VoIP, ed è un attacco solitamente portato ai servizi di messaggistica istantanea e a programmi che sfruttano il VoIP. Gli attacchi sono più semplici rispetto a quelli basati sul phishing essendo questa un campo ancora poco esplorato e la gente non è ancora pienamente sensibilizzata sul problema. Hanno lo stesso scopo del phishing, vale a dire quello di sottrarre informazioni personali al fine di poterle usare a proprio vantaggio. Per portare a termine tali attacchi il pirata informatico può usare messaggi preregistrati che vengono inviati agli utenti sperando che questi rispondano inviando tali informazioni.

2.Cos'è una Botnet

2.1 Definizione

Tra le minacce che si possono diffondere e che possono aggredire la rete c'è sicuramente da tenere in considerazione quella rappresentata dalle Botnet. Secondo un report di McAfee sull'andamento dei malware si può notare un aumento del 141% nell'anno 2009 a partire dal mese di marzo, ma anche l'espandersi delle Botnet. Oltre 14 milioni di computer sono stati colpiti da una Botnet e il numero di minacce di questo tipo continua a crescere vertiginosamente il che dipende soprattutto dalla cattiva protezione dei computer presenti nelle nostre case, infatti in media oltre 150.000 computer vengono infettati quotidianamente da questo tipo di malware. L'espansione di Botnet rappresenta inoltre il motore principale della crescita di volume di spam, che è ora al 92% di tutte le e-mail. I volumi di spam hanno ora superato del 20% i record più elevati, crescendo a una velocità costante di circa il 33% ogni mese. In altri termini, i volumi di spam crescono di oltre 117 miliardi di email ogni giorno. Secondo il sito http://www.techterms.com/ una Botnet è "*un gruppo di computer controllati da una singola sorgente ed esegue programmi e script collegati al software*". Tali computer sono spesso denominati Bot o computer zombie e sono completamente assoggettati al volere del loro creatore e sempre pronti ad eseguire qualsiasi comando gli venga impartito. Questo tipo di rete riesce a portare attacchi che risultano sicuramente tra i più pericolosi e più efficaci della rete, anche in termini di guadagno economico. Una rete del genere viene creata da un hacker che progetta un apposito programma e lo invia attraverso diversi canali della rete, che possono essere canali IRC, HTTP o anche altri canali di tipo P2P. Il programma che viene inviato agli utenti è detto Bot ed ha la capacità di essere eseguito automaticamente ed in maniera del tutto autonoma sul computer che si intende infettare. Tali reti non solo riescono ad infettare in maniera completamente nascosta gli altri terminali, ma riescono anche a rendere difficilmente rintracciabile l'aggressore in modo che non possa essere localizzato dai computer che vengono infettati. Talvolta ci si riferisce al terminale infettato con il nome di *Bot* o anche con quello di *Zombie*. Anche se

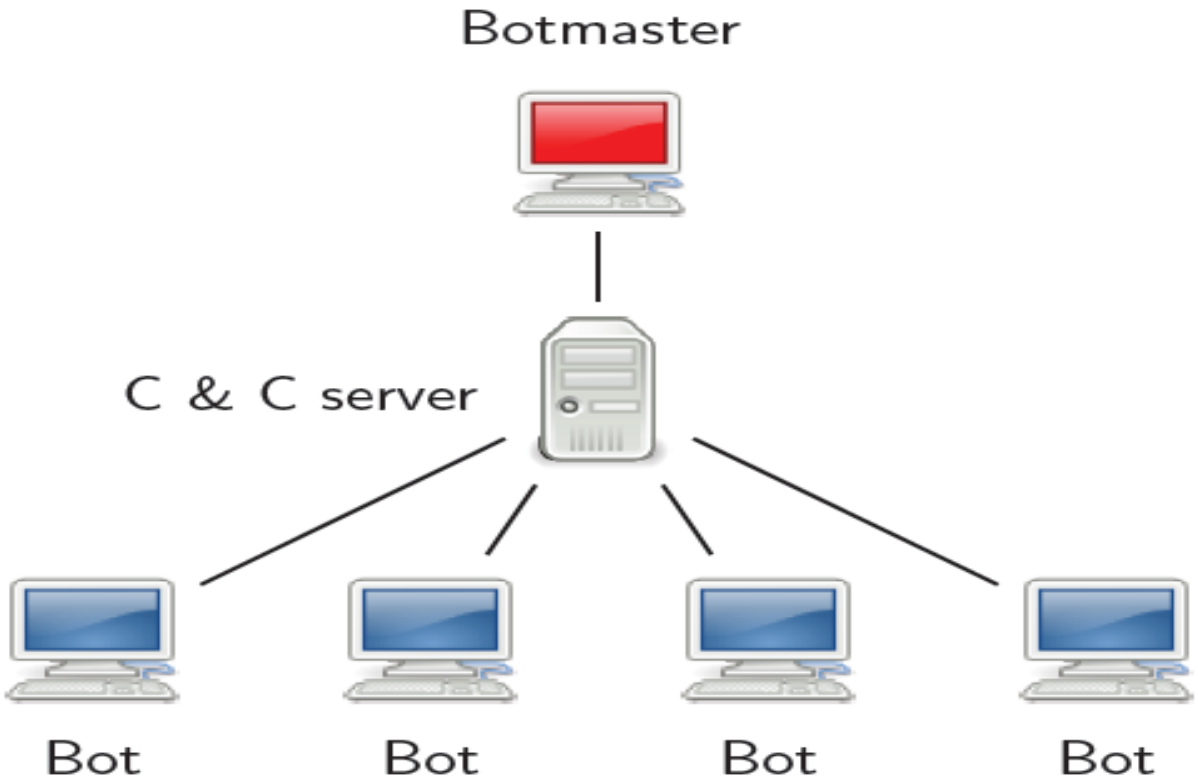
ad uno sguardo più superficiale potrebbe sembrare che l'unica motivazione che un hacker dovrebbe avere per creare una rete del genere sia quello di dimostrare di essere talmente in gamba da riuscire a penetrare tutte le difese presenti sui vari computer della rete. Se invece non ci soffermiamo solo alla superficie ma effettuiamo un'analisi più approfondita riusciamo a notare che negli ultimi anni il numero delle Botnet è in crescente aumento e si può notare che questo aumento è dovuto soprattutto a forti interessi economici che vanno crescendo sempre di più col passare del tempo. Inizialmente reti del genere venivano sfruttate soprattutto per mandare messaggi di spam in maniera contemporanea e verso un numero di computer sempre crescente, col passare del tempo ci si è accorti che le aziende, che adoperavano un sito web come mezzo per il loro commercio, potevano mettere fuori combattimento altre aziende concorrenti proprio servendosi della massiccia quantità di messaggi che queste reti riescono a mandare simultaneamente. L'errore più comune che ciascun utente possa commettere è quello di sottovalutare la potenza di queste reti e le molteplicità dei loro scopi, i proprietari infatti non cercano soltanto di colpire reti strettamente commerciali e ma tutti i tipi di terminale e quindi il rischio di contaminazione non decresce solo perché il terminale non appartiene ad una rete commerciale. Basti solo considerare che i nodi di una tale rete possono avere compiti variegati e quindi ci si potrebbe servire di tali computer per aumentare il traffico sulla rete o magari anche come ponte verso altri terminali fino a quel momento irraggiungibili.

La falla di cui approfittano gli hacker per tentare la contaminazione è tra quelle che di solito vengono identificate tra quelle del browser o del sistema operativo, in questo modo il server attaccante riesce a penetrare nella macchina e ad installare il codice malizioso. Un effetto immediato della corretta installazione del Bot sul computer bersaglio è sicuramente l'improvviso riavvio del sistema, ciò permetterà al virus di installarsi all'avvio e di essere riconosciuto come libreria di sistema e quindi di non essere identificato dagli antivirus e di poter funzionare da *entrata di servizio* per il sistema infetto. Una volta contaminato il computer entrerà a far parte della rete controllata dall'hacker che assegnerà ad ogni nuova macchina un identificativo unico. Tutti i terminali infettati verranno controllati e gestiti tramite un apposito software, come Neosploit, che potrà anche essere utilizzato per impartire ordini.

2.2 Anatomia di una Botnet

Abbiamo sinora parlato di queste nuove e pericolosissime reti che si stanno espandendo sempre più velocemente, ci occuperemo ora della descrizione dettagliata gli elementi principali di cui tali reti sono composte. Le entità principali che compongono una Botnet, sono:

1. Botmaster
2. Unità di Comando e Controllo
3. Canale di Comunicazione
4. Bot o Zombie



Il Botmaster: Spesso conosciuto anche come BotHerder, è la persona o il gruppo di persone che si è occupa di controllare i Bots remoti[17]. Ha inoltre il compito di progettare e scrivere il malware con il compito di infettare e assoggettare gli altri computer e si preoccupa di correggerne gli errori. Un vantaggio molto importante di cui il master può usufruire è quello di poter lanciare i suoi attacchi alla rete senza la necessità di dover avere una posizione prefissata. Ciò comporta che il malintenzionato può trovarsi in qualsiasi punto che risulti più sicuro e più difficilmente raggiungibile. Solitamente viene scelto un luogo che sia abbastanza distante dal punto della rete in cui è avvenuta la ricezione del Bot e quindi colui che ha lanciato l'attacco non è rintracciabile. Altra caratteristica che contraddistingue il Master è quella di riuscire a cambiare indirizzo IP più volte durante l'arco della giornata in modo da non essere identificato dagli altri computer della rete ed essere così ancora più protetto da eventuali hacker che potrebbero voler introdursi nella sua rete per sfruttare i computer zombie.

Centro di Comando e Controllo: costituisce il vero centro di controllo della Botnet ed ha molteplici compiti, tra i quali:

- Si occupa di allertare tutti i computer zombie che fanno parte della Botnet
- È il nodo per cui passano tutti gli ordini del Master che verranno poi comunicati ai computer infettati
- Ha l'importantissimo compito di schermare il Master all'interno della rete così da renderlo irrintracciabile anche dall'interno della stessa. Come si riesce ad evincere dai suoi compiti, tale unità ha un ruolo centrale all'interno delle reti di questo tipo. Tra le varie cose che potrebbero caratterizzare una unità di controllo rispetto ad un'altra ci sono sicuramente il mezzo fisico attraverso il quale si comunica con i computer che fanno parte della rete e le modalità di trasferimento degli ordini dal Master ai computer zombie. La prima distinzione che viene fatta è sul metodo usato per controllare i Bot. Si possono distinguere due categorie:

1. **Controllo Centralizzato**
2. **Controllo Distribuito**

A ciascuna di queste tipologie di centro di controllo è associata una particolare metodologia per lo scambio dei messaggi. Quelle che abbiamo individuato sono:

- **Push:** Questo tipo di tecnica fa sì che tutti i computer zombie della rete restino in uno stato di standby finché il master non decide di allertarli inviando loro l'ordine da eseguire.
- **Pull:** Questa tecnica ha un approccio differente dalla precedente infatti, non lascia i computer infettati inattivi, ma fa in modo che i Bot interroghino continuamente il master per sapere se egli ha ordini da svolgere per loro.

I centri di controllo di tipo centralizzato utilizzano una tecnica di comunicazione di tipo Push ed utilizzano canali di comunicazione molto comuni, come per esempio:

- **IRC**: è il canale di comunicazione più diffuso e più classico dato che rappresenta la più antica forma di chat online. Esso è considerato sicuramente il mezzo di comunicazione più amato dagli hacker, basta immaginare che in una chatroom si possono trovare migliaia di utenti, che potrebbero essere in realtà potenziali zombie e il Master potrebbe utilizzare la chat per poter dialogare con i suoi zombie e impartire loro un comando semplicemente scrivendolo nella chatroom. Un ordine dato dal Botmaster in questa maniera riesce ad allertare immediatamente tutte le migliaia di zombie connessi alla chat.

- **HTTP:** questo canale costituisce una variante un più scomoda di IRC, ma possiede il grande vantaggio di non essere filtrato dai firewall e quindi di permettere al Botmaster di poter portare attacchi più facilmente grazie a questo protocollo. Nella maggior parte dei casi il Botmaster gestisce la Botnet attraverso una pagina web da dove è in grado sia di controllare tutti

gli aspetti della Botnet e soprattutto di ordinare agli zombie appartenenti alla rete di attaccare.[12]

- **P2P**: Appartiene alla classe dei nuovi mezzi di comunicazione che possono essere utilizzati dalle Botnet. Si sfrutta la popolarità che tale canale ha acquisito in questi anni. I Botmaster potrebbero nascondere i Bot tra i file comuni e riuscire, tramite i programmi che usano questo protocollo di comunicazione, ad installare i programmi che hanno il compito di infettare. Un utente non eccessivamente attento potrebbe essere costretto ad installarli sulla propria macchina entrando così a far parte della rete.[7]

Abbiamo accennato che con la parola Bot possiamo indicare sia il computer contaminato che il programma che è stato utilizzato per contaminarlo. Per quanto riguarda il primo aspetto della questione, i terminali contaminati sono comunissimi personal computer che tipicamente montano un sistema operativo Microsoft che risulta il più semplice da attaccare proprio a causa delle sue falle di sicurezza. Ultimamente però, sono stati creati anche dei worm capaci di penetrare sistemi operativi storicamente considerati inattaccabili, quali Linux e Mac OS X. Anche in questi sistemi operativi sono state individuate delle falle di sicurezza che possono rendere più semplice e meno ardua la contaminazione. I Bot si occupano, tra le altre cose, anche di raccogliere informazioni per i motori di ricerca e siti di shopping. Avendo queste capacità i Bot vengono spesso usati per apportare attacchi di tipo DoS contro siti web oppure si possono occupare di fare phishing o migliaia di mail di spam sulla rete.

Per quanto riguarda invece la seconda accezione con la quale viene usato questo termine, si può dire un Bot è un tipo di malware che permette al Botmaster della rete di terminali compromessi di completare un attacco al computer i cui possessori sono ignari degli effetti derivanti. Tra i vari tipi di Bot che possono infettare un computer, i più usati sono:

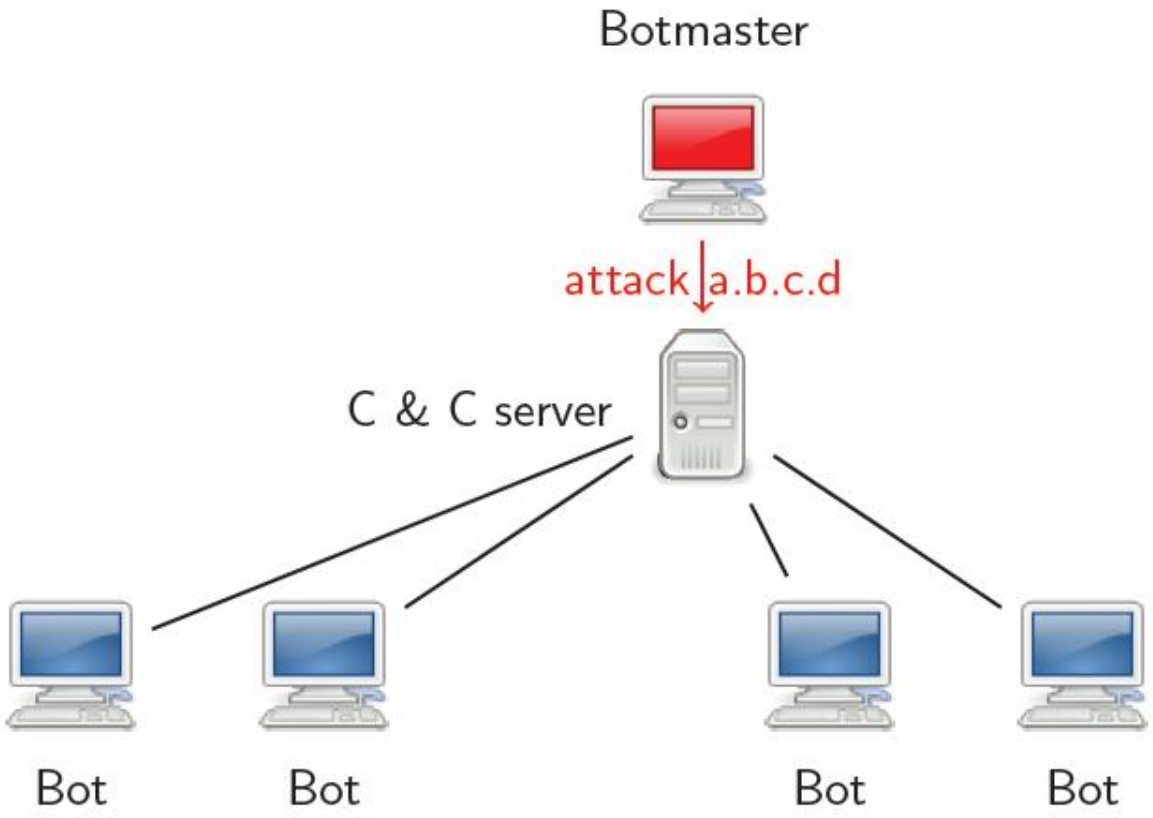
- **XtremBot, Agobot, Forbot, Phatbot:** A questa famiglia appartengono i Bot al momento più conosciuti, e ne sono presenti sulla rete più di 500 versioni differenti. Il codice sorgente è scritto in C++ e viene rilasciato sotto GPL. Il loro design può variare da singolo livello di astrazione ad uno più astratto basato su un approccio modulare al quale si possono aggiungere scanner per migliorarne l'efficienza nello sfruttamento delle vulnerabilità. Possono utilizzare anche la libreria libpcap utile per lo sniffing dei pacchetti. Gli Agobot forniscono molti meccanismi per nascondere la loro presenza sul computer ospite, come meccanismi che alternano il flusso di dati su NTFS, Killer di Antivirus ed inoltre meccanismi di crittografazione polimorfica. Questo tipo di Bot offre al Botmaster anche meccanismi di sniffing del traffico e di ordinamento e hanno la possibilità di sfruttare altre vie di comunicazione.
- **UrXBot, SDBot, UrBOt, RBot:** Anche questo tipo di Bot viene rilasciato sotto GPL, ma diversamente dal tipo precedente di Bot hanno un design meno astratto e vengono principalmente scritti in linguaggio C. Nonostante il loro design sia meno sofisticato, questo tipo di Bot sono largamente conosciuti ed usati su Internet. Diversamente dagli Agobot il loro codice non è molto chiaro e il software ha un numero alquanto limitato di caratteristiche.
- **GT-Bots e Bots basate su mIRC:** questo tipo di Bot circola sulla rete in molteplici versioni, la principale motivazione è soprattutto perché mIRC è uno dei client IRC più diffusi per Windows. I GT-Bot sono worm creati esclusivamente per questo client IRC e proprio attraverso questo programma di chat il Botmaster riesce a lanciare una serie di file binari, di solito con l'estensione DLL. Questo tipo di Bot viene di solito corredato di meccanismi di controllo che rendono l'esecuzione di mIRC nascosta allo stesso sistema operativo Windows e magari riescono ad influenzare l'host in vari aspetti.
- **DSNX:** Data Spy Network X è scritto in C++ e si può ottenere il codice sorgente disponibile su licenza GPL. La particolarità di questo Bot è che si riescono ad aggiungere nuove funzionalità molto facilmente grazie all'architettura a plug-in.
- **Bot Q 8:** Sicuramente sono i più leggeri della categoria. Sono costituiti solitamente da sole 926 linee di codice scritte solitamente in C++. Questo Bot è usato principalmente per l'infezione dei sistemi che utilizzano Linux e

una volta scaricati riescono ad aggiornarsi automaticamente a versioni più recenti tramite un semplice download fatto tramite il protocollo HTTP.

- **Kaiten:** Il suo scopo principale è quello di attaccare sistemi Linux e Unix e a differenza degli altri tipi di Bot possiede una shell remota che viene solitamente utilizzata dall'hacker per cercare altre vulnerabilità del sistema appena infettato oppure possono permettere una esplorazione dell'host da remoto. Questo tipo di programma ha però una debolezza che si trova nel suo stesso schema di autenticazione che è facile da attaccare ed eludere.
- **Perl Bot:** L'ultima famiglia di Bot include quelli basati sul linguaggio di programmazione Perl. Anche questi Bot sono molto piccoli ed hanno un corpo costituito solo da poche centinaia di linee di codice. Dato il loro peso ridotto, ovviamente riescono ad offrire comandi rudimentali, principalmente per permettere l'esecuzione di attacchi DDoS e sono principalmente usati per la contaminazione di sistemi Unix-based. [39]

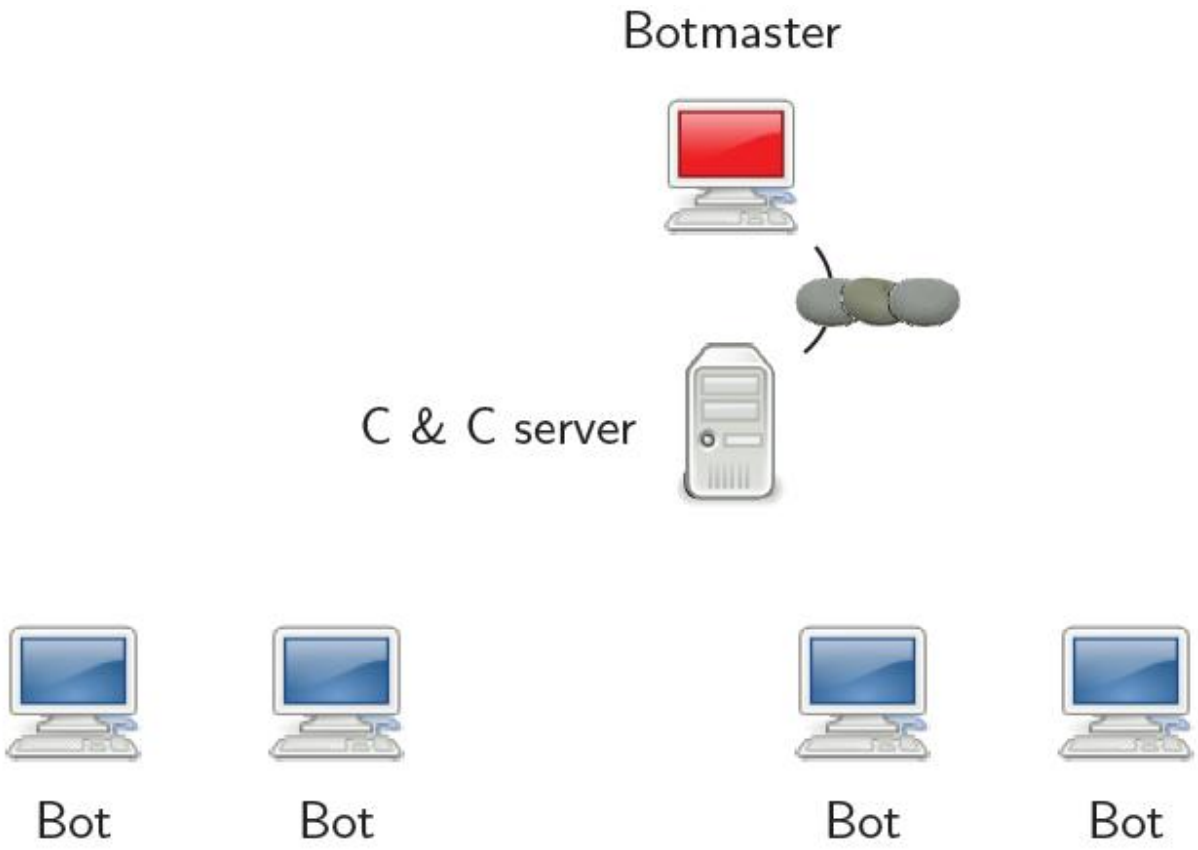
2.3 Funzionamento di una Botnet

Dopo aver descritto in maniera approfondita i vari componenti che costituiscono una Botnet passiamo ora ad analizzare il loro comportamento e come interagiscono tra di loro. Da come abbiamo precedentemente visto il Botmaster non invia gli ordini ai Bot direttamente ma si serve del Centro di Comando e Controllo come tramite per inviarli. Un problema che potrebbe sorgere sarebbe quello che i client della Botnet potrebbero connettersi e disconnettersi continuamente e quindi magari alcuni comandi inviati dal Botmaster non vengano effettivamente ricevuti da tutti gli zombie. Quando si invia un comando al C&C, di solito, può anche specificare i Bot che lo devono eseguire.

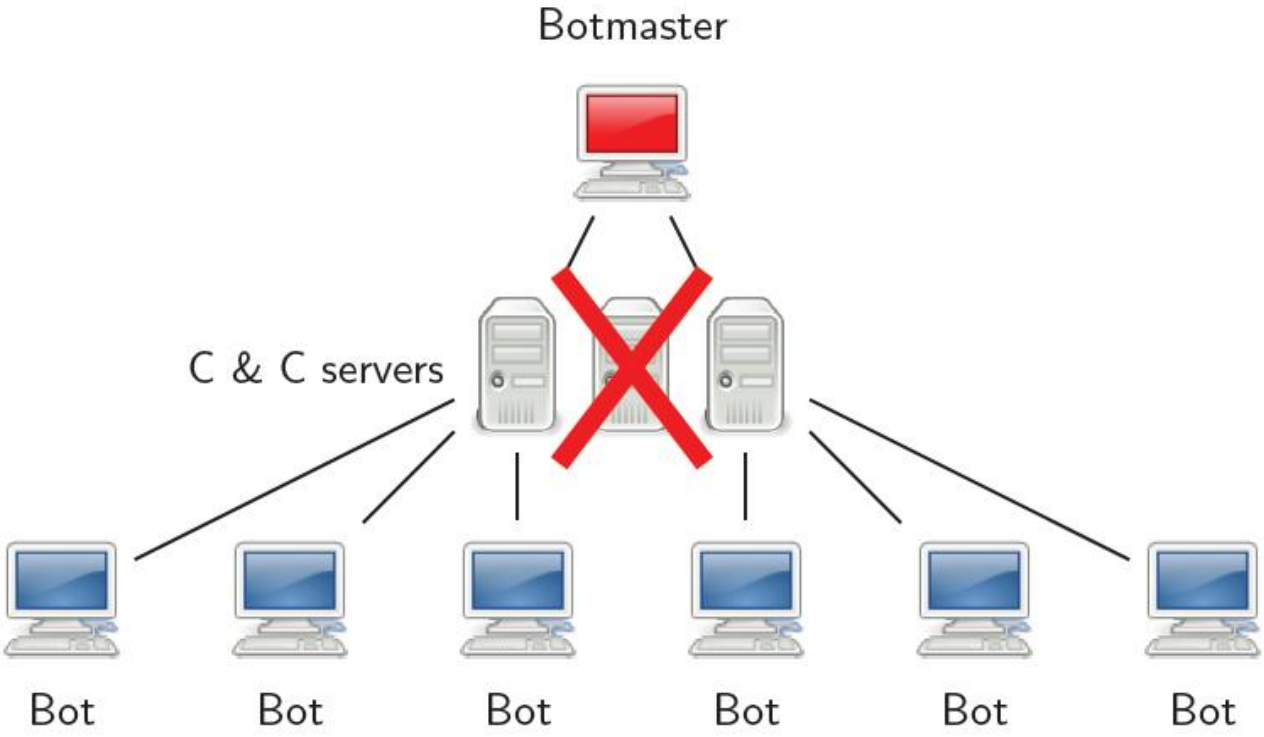


Sarà poi compito del server C&C inoltrare il comando ricevuto ai vari Bot destinatari. Come abbiamo accennato in precedenza il server ha l'importantissimo compito di rendere non rintracciabile il Botmaster e questo è

possibile tramite l'offuscamento del canale di connessione che esiste tra il suddetto server ed il Botmaster.

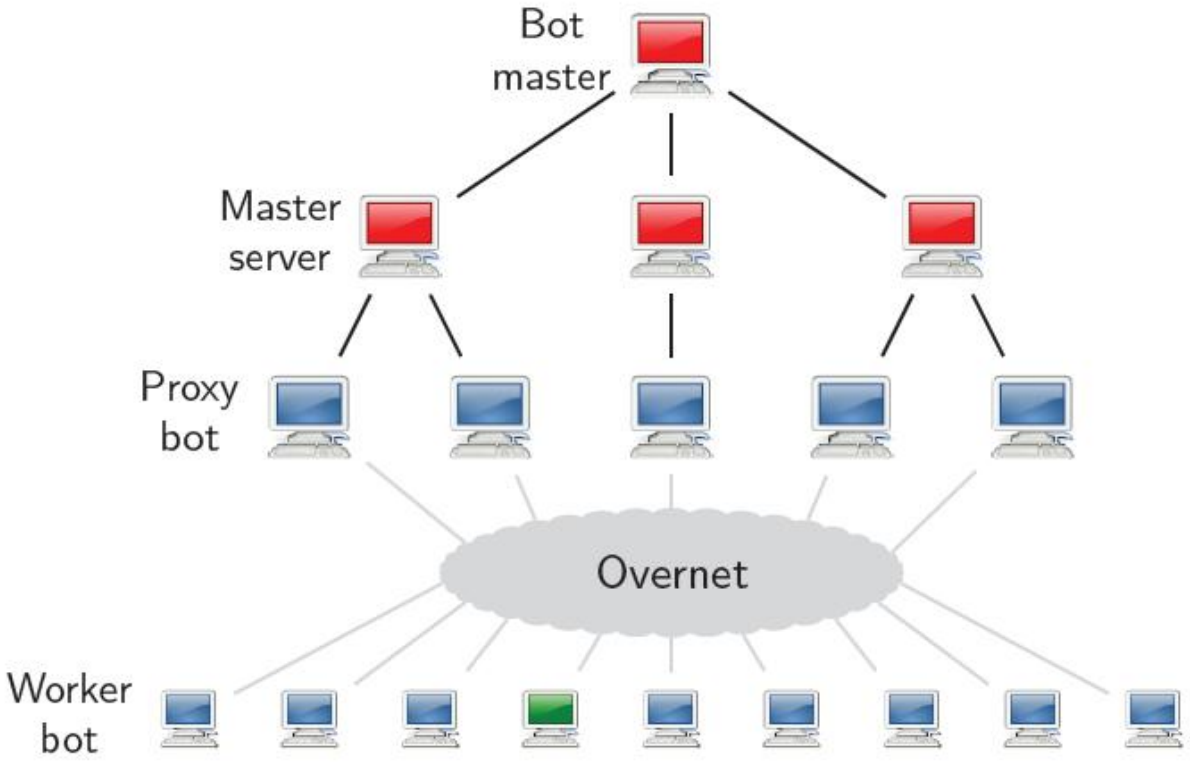


Dato il suo ruolo di controllore della rete di Bot questo fa sì che questo sia un punto di grande importanza per la Botnet, ma molto spesso tale server è costituito da un'unica macchina e questo sicuramente costituisce un possibile punto debole visto che essendo il server unico nel caso venisse danneggiato o addirittura eliminato si perderebbe il controllo totale su tutti i Bot della rete. Siccome questo costituirebbe una perdita di utili per il Botmaster, la soluzione più semplice sarebbe quella di sostituire l'unico server con più server in modo tale che nel caso uno di questi venisse danneggiato o eliminato dalla rete i terminali ad esso connessi non si ritroverebbero *orfani* del server, ma si potrebbero appoggiare agli altri server disponibili e questo riuscirebbe ad ovviare il problema evidenziato evitando così al Botmaster di avere perdite economiche.



La stessa modalità di funzionamento viene usata dalle reti che invece di sfruttare il canale di comunicazione IRC utilizzano per comunicare il canale HTTP. Le uniche differenze sono nella modalità di comunicazione con gli zombie che in questo caso sarà di tipo *pull,* cioè sarà compito dei Bot contattare ripetutamente il Botmaster per sapere se vi sono nuovi ordini. Diversamente dal traffico di tipo IRC, che da qualche tempo a questa parte viene analizzato più attentamente per via di tutti i malware che esso può trasportare, il traffico HTTP malevolo può essere più spesso confuso con quello benigno di cui l'utente ha fiducia e questo porta il bot ad essere trasmesso e scaricato più facilmente, anche grazie al fatto che è molto più difficile bloccare il traffico a livello di DNS.

Per quanto riguarda invece le Botnet che attaccano il traffico P2P anche la struttura cambia in maniera sostanziale, come ci viene mostrato dalla figura sottostante.



In una Botnet P2P non c'è un server centrale ma i Bot sono connessi tra di loro e possono ciascuno comportarsi come server C&C e come client. Sono solitamente più robuste e rendono la difesa della comunità molto più ardua. Il ciclo di vita di una Botnet di questo tipo è composto da 3 stadi:

1. Reclutare membri Bot: Le reti P2P stanno guadagnando popolarità ma non sempre si è certi che i file scambiati non siano maliziosi. È tipico degli attaccanti identificare gli host vulnerabili in una rete P2P esistente che potrebbero diventare futuri zombie di una Botnet e la taglia di questa è sicuramente limitata dalla taglia della rete P2P e la rete sarà solo un mezzo per la propagazione. Inoltre la contaminazione tramite più mezzi di diffusione rende il reclutamento di altri bot più flessibile e pratico.
2. Formare la Botnet: Dopo l'infezione la cosa importante è quella di non lasciare che i terminali infettati restino isolati ma che si connettano ad altri host infettati e soprattutto al Botmaster. Vi sono tre classi a cui queste reti potrebbero appartenere:
    a. *Parasite*: Si utilizzano gli host compromessi all'interno della rete P2P che si sta utilizzando per inoltrare i comandi.

i. *Leeching*: In una rete di questo tipo sono gli host a connettersi alla rete P2P per ricevere i comandi dal server C&C. In questo caso gli host possono appartenere o meno a tale rete P2P.
ii. *Bot-only*: Questa botnet costruisce la sua rete in cui tutti i membri sono bot.

Un host compromesso deve sapere come partecipare alla Botnet. La prima azione da fare è sicuramente la fase di bootstrap che può essere adottato per la costruzione della rete. Per questo motivo c'è bisogno che di codificare all'interno del worm stesso la lista di peer da contattare subito dopo l'avvenuta contaminazione.

3. Attendere in attesa di istruzioni: Una volta che la rete è stata costruita tutti i Bot attendono le istruzioni per svolgere azioni illecite o magari aggiornamenti. Il C&C è una parte importante del design di una rete e decide le modalità di comunicazione della rete e ne caratterizza quindi la robustezza contro i vari fallimenti, il monitoraggio della sicurezza e anche le difese di tale rete.

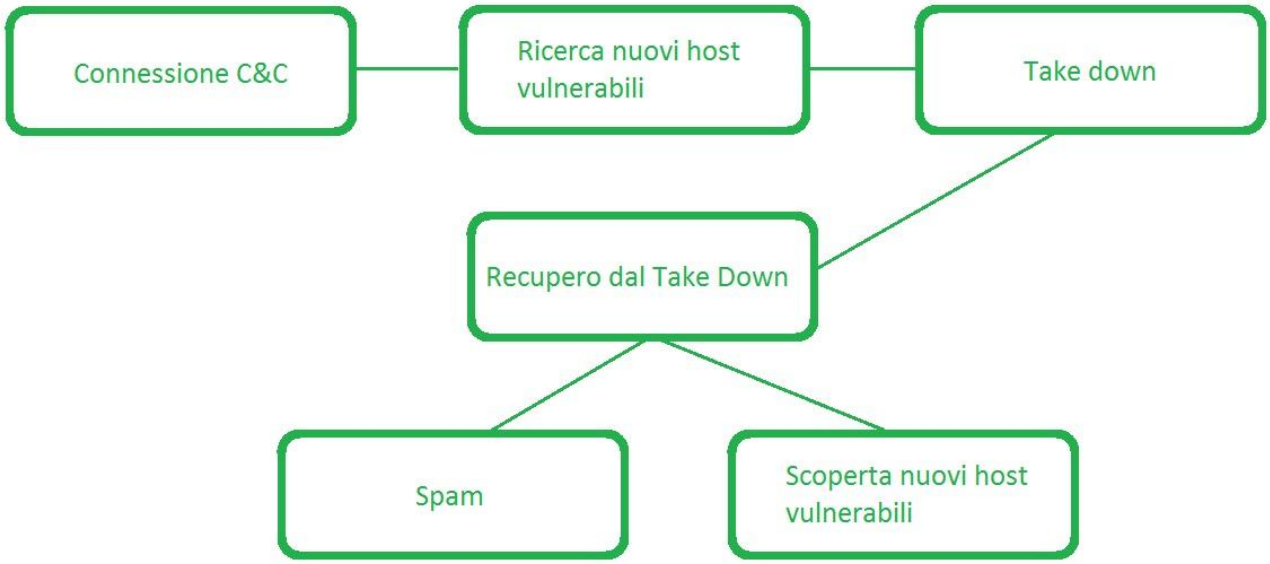
L'interesse si è spostato su questo canale proprio perché i protocolli P2P sono stati testati dalle applicazioni di file sharing che le hanno rese meno soggette ad errori ed hanno proprietà che migliorano le prestazioni stesse di Internet.

In questo tipo di Botnet un ruolo fondamentale viene svolto dai Proxy, infatti tali componenti costituiscono il punto di incontro tra i Bot e il Botmaster e soprattutto si preoccupano di fare da tramite tra questi e i cosiddetti Worker Bot rendendo così nascosto e protetto il controllore della rete. I Bot si occupano di ricercare le chiavi nella rete P2P che serviranno a localizzare i proxy all'interno della rete e dopo essersi autenticati sul proxy i Bot restano in attesa di ricevere i comandi inviati dal proxy. Come precedentemente accennato il proxy si occupa di fare da tramite tra il Botmaster e i workers comunicando a questi ultimi i comandi da eseguire.

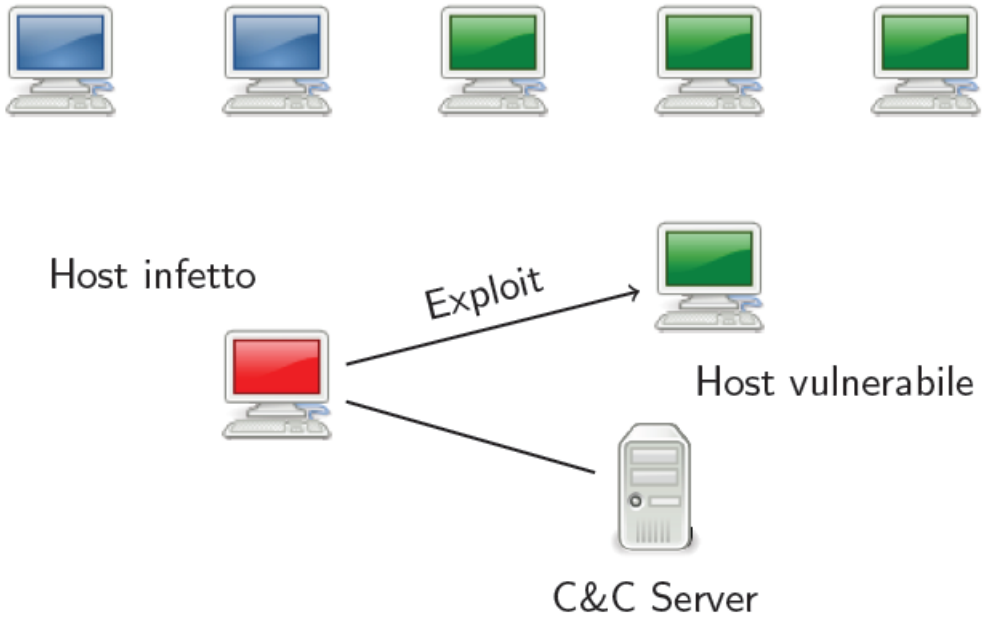
Un altro argomento sicuramente interessante da affrontare è costituito dal ciclo di vita di un Bot, in pratica ci occuperemo principalmente di tutto quello di cui un host infetto deve occuparsi dal momento in cui entra a far parte della rete.

2.4 Ciclo di vita di un Bot

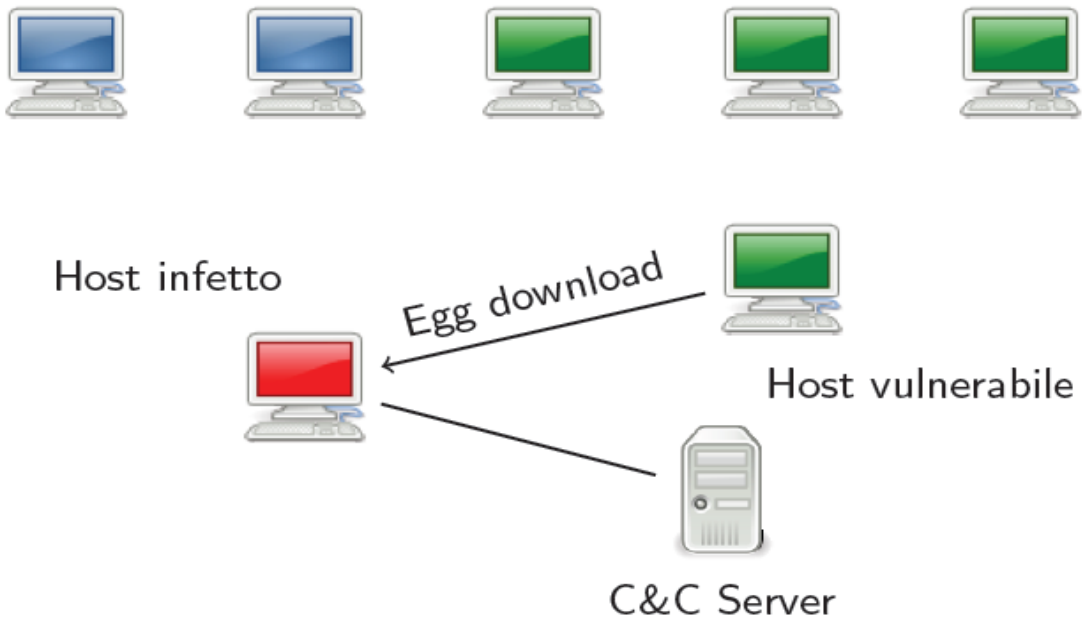
Vediamo ora come si comporta uno zombie dal momento in cui è stato appena contagiato dal codice malevolo fino a diventare pienamente parte della rete. Il ciclo di vita di un tale host può essere riassunto tramite il seguente schema.



L'attacco viene fatto partire dal C&C della Botnet che si occupa di fare un port scan per trovare le nuove vittime che non hanno difese che risultino difficili da oltrepassare. Questa ricerca può partire da tutti gli host che fanno parte della rete che hanno il compito di mandare un Exploit a tutti i computer a loro collegati. [18]

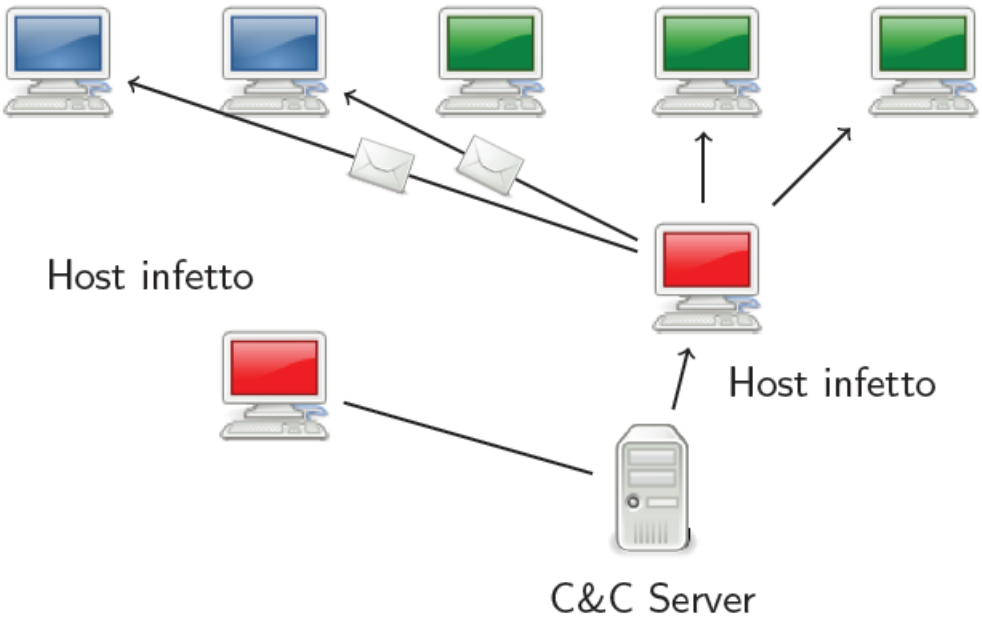


Un exploit è un software che riesce ad oltrepassare le difese di un altro computer e riesce a fornire un accesso a tale macchina anche da remoto, garantendo inoltre privilegi di amministratore all'attaccante. Dopo aver mandato l'Exploit la vittima manda una richiesta di download di un rootkit o del Bot stesso, spesso denominato Egg.



Una volta avvenuta l'installazione di tale software la macchina si connetterà direttamente al C&C server completando così un vero e proprio Bot della rete.

A questo punto tale macchina potrà essere utilizzata sia come ponte per ricercare altre macchine vulnerabili da poter infettare oppure può attaccare insieme alle altre macchine.



3.Attacchi di una Botnet

Dopo esserci occupati del funzionamento di una rete di questo genere occorre fare una panoramica molto generica sui tipi di attacchi che più comunemente queste reti possono portare sia agli utenti che ai siti Internet. Tra i possibili attacchi ne evidenziamo i più importanti:

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

3.1 Dos

Tale tipologia di attacco è sicuramente quella più efficace tra quelli eseguibili da una Botnet. È un tentativo di rendere una risorsa su un computer non disponibile per un utente. Sebbene gli obiettivi di un tale attacco possono variare, di solito si preferiscono servizi o indirizzi Internet che il Botmaster vuole rendere non funzionanti efficientemente per un determinato periodo di tempo o magari per sempre. I bersagli che si preferisce colpire sono principalmente tutti quei servizi offerti dai server di alto profilo, come possono essere quelli utilizzati dalle banche, i gateway per i pagamenti tramite carta di credito o anche i Root name server. La più comune metodologia di attacco utilizzata per riuscire ad abbattere questi sistemi richiede la saturazione delle risorse tramite un ampio insieme di richieste esterne mandate da ciascun Bot della rete, in modo che il server non riesca a rispondere in maniera corretta a tutte le richieste o quantomeno non lo riesca a fare velocemente. Questi attacchi hanno lo scopo sia di costringere il server bombardato ad un riavvio forzato, e sia di sprecare la risorsa messa a disposizione talmente tanto da non permettere al server il soddisfacimento di altre richieste ad esso inviate. Si potrebbe inoltre tentare di saturare il canale di comunicazione tra l'utente e la vittima in modo da rendere il server irraggiungibile per un lungo periodo di tempo. Un attacco di tipo Denial of Service è un tentativo esplicito di causare un disservizio facendo in modo che utenti realmente interessati non possano usufruire di tale funzionalità. I principali obiettivi di questi attacchi sono solitamente tutti i dispositivi di rete inclusi a quelli per il routing e web, email, o server DNS. Vi sono vari modi per effettuare un attacco DoS e i 5 basilari sono:

- Consumo di risorse computazionali quali: ampiezza di banda, spazio su disco, tempo di processore.
- Sconvolgimento di alcune informazioni di configurazione, come ad esempio quelle utili per il routing.
- Sconvolgimento delle informazioni sullo stato, come un insolito reset di sessioni TCP.
- Sconvolgimento di componenti fisici della rete.

- Ostruzione del mezzo di comunicazione che c'è tra gli utenti predisposti e la vittima in modo tale che essi non riescano più a comunicare in maniera adeguata.

Abbinate a queste tecniche si può sicuramente includere l'esecuzione di malware che abbiano lo scopo di:

- Usare al massimo il processore, in modo da evitare che qualsiasi altro lavoro possa essere svolto
- Insinuare errori nel microcodice della macchina
- Insinuare errori nell'esecuzione sequenziale di istruzioni in modo da forzare il computer ad uno stato instabile o di blocco.
- Sfruttare gli errori nel sistema operativo per causare starvation delle risorse in modo tale che nessun lavoro reale possa essere compiuto.
- Fare in modo che lo stesso sistema operativo abbia dei crash.
- IFrame, in cui un documento HTML è fatto per visitare una pagina web con molti Kb di informazioni finché non raggiunga il limite di visite per fare un modo che si ecceda il limite di ampiezza di banda.

Questo tipo di attacco può anche essere fatto in modo distribuito e ciò avviene quando una molteplicità di sistemi compromessi inonda la banda o le risorse del sistema bersagliato, di solito uno o più web server, che viene compromesso tramite una serie di metodi. Il meccanismo di attacco può essere portato stesso dal malware (es. MyDoom) solitamente innescato in una data e un'ora prestabilita e l'indirizzo IP è codificato nel malware e quindi non si ha bisogno di nessun'altra interazione per lanciare l'attacco. Il principale vantaggio derivante da questo attacco è che più macchine riescono a generare più traffico simultaneamente e sono, oltretutto, più difficile da rendere inoffensive.

3.2 Adware

Il termine **adware** (in inglese, contrazione di *advertising-supported software*, cioè software sovvenzionato dalla pubblicità) indica una modalità di licenza d'uso dei programmi software e prevede la presentazione all'utente di messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. I programmi definiti adware sono provvisti di un contratto di licenza d'uso consultabile dall'utente; in certi casi, però, questo contratto è reso dai produttori spropositatamente lungo e soprattutto viene spesso presentato con linguaggio vago e fumoso, con la conseguenza che molti utenti procederanno con l'installazione senza aver ben compreso i termini di licenza. Tali programmi presentano rischi per la stabilità e la sicurezza del computer: alcuni di essi possono aprire continuamente popup pubblicitari che rallentano notevolmente le prestazioni della macchina, altri possono modificare le pagine html direttamente nelle finestre del browser per includere link e messaggi pubblicitari propri, con la conseguenza che all'utente viene presentata una pagina diversa da quella voluta dall'autore. Non è facile, ed a volte quasi impossibile, essere a conoscenza di quali dati vengano inviati e ricevuti attraverso tale connessione, dati che possono essere potenzialmente dannosi se ricevuti o che violano la privacy se inviati.

3.3 Spyware

Uno spyware non è altro che un malware che viene installato sui computer per raccogliere informazioni sulla navigazione Internet degli utenti senza che loro lo sappiano. Tipicamente lo spyware viene installato in maniera segreta sul computer dell'utente oppure su computer pubblici con lo scopo di monitorare segretamente tutti gli utenti che utilizzano quel computer. Ma le funzioni di uno spyware si estendono ben oltre il semplice monitoraggio, difatti, uno spyware può anche interferire con il controllo dell'utente in vari modi, potrebbe ad esempio installare software addizionali e potrebbe reindirizzare il browser ad altre pagine. Uno spyware può anche cambiare le impostazioni del

computer per far risultare la connessione del pc lenta, cambiare la home page del browser o limitare le funzionalità di altri programmi. Solitamente un programma è soggetto a più di un'infezione anche se di solito questa non avviene tramite un altro host infetto, ma viene di solito installato insieme ad altri programmi di cui l'utente necessita e ciò causa un degrado delle prestazioni del computer e soprattutto comportamenti non voluti sia che riguardino l'attività di CPU, l'uso del disco o il traffico di rete. In molte infezioni gli spyware non risultano evidenti e infatti molto spesso gli utenti attribuiscono la particolare lentezza a questioni hardware, problemi di installazione di Windows o altri tipi di infezioni, portando spesso gli utenti a comprare un nuovo computer. Gli spyware riescono a collaborare tra di loro creando poi gli effetti sinora descritti ed inoltre riescono a disabilitare firewall e antivirus, aggiungere o eliminare impostazioni di sicurezza sui browser così da indebolire le difese del sistema.

3.4 Email Spam

Lo spam tramite email può essere considerato un sott'insieme che coinvolge messaggi identici mandati a numerosi destinatari. Il numero di email di spam è aumentato esponenzialmente sin dai primi anni '90 ed è arrivato ad svariati miliardi (oltre 100 nel 2008). Ultimamente però questo numero di email è andato sempre più diminuendo a causa del filtro che molti utenti oramai applicano alle loro mail. Di queste mail di spam circa l'80 % viene mandato da terminali che fanno parte di una Botnet. Gli indirizzi ai quali mandare le mail di spam vengono recuperati da chat, siti web, liste di clienti, newsgroup e soprattutto da virus il cui unico scopo è quello di sottrarre le rubriche degli utenti infettati. Si possono avere 2 tipi particolari di spam:

- **Unsolicited bulk email**: sono messaggi di email non richiesti che vengono inviati in massicce quantità.
- **Unsolicited commercial email**: questa è una definizione più restrittiva è utilizzata dai regolatori che regolano il commercio.

Descriveremo ora le diverse tecniche utilizzabili per fare spam:

- **Appending:** è un processo di merge di due diversi database contenenti, il primo le informazioni sui clienti dell'azienda come nome, indirizzo e numeri di telefono, mentre il secondo, solitamente fornito da service provider, contiene email di molte migliaia di utenti. Questa operazione ha lo scopo di individuare le corrispondenze tra i database e quindi abbinare le informazioni dei clienti alle email.
- **Image Spam:** Metodo di offuscamento in cui il testo del messaggio viene inviato come immagine in modo che il testo non possa essere identificato da eventuali filtri.
- **Blank Spam:** Viene inviato il messaggio senza il carico dell'annuncio, infatti spesso tale messaggio è completamente vuoto e viene catalogata come spam perchè viene comunque considerato come carico non richiesto.
- **Backscatter spam:** è un effetto scaturito direttamente dalle email di spam, dai virus e dai worm e consiste nel far mandare ai mail servers dei bounce message ai vari utenti.

3.5 Access Number Replacement

Lo scopo di questo attacco è sicuramente quello di infastidire a tal punto l'utente da costringerlo a cambiare il suo numero di telefono. L'hacker sostituisce il numero di un qualsiasi provider Internet con quello della vittima, facendo in modo che egli venga bombardato dalle chiamate di tutti gli utenti che si servono di quel provider per connettersi ad Internet. L'utente verrà così costretto a cambiare numero di telefono per evitare di essere continuamente disturbato.

3.6 Fast Flux

Questa tecnica basata sul DNS ed è usata dalle Botnet per nascondere i siti che rilasciano malware e il phishing dietro una rete di host compromessi che si comportano come proxy e che sono in continuo cambiamento. Lo stesso termine si può anche riferire alla combinazione tra reti P2P, sistemi command&control distribuiti, load balancing del web e redirezione di proxy utilizzate per rendere le reti di malware più resistenti rispetto alla loro individuazione ed alle contromisure. La Botnet più famosa che fa utilizzo di questa tecnica è la Storm. Gli utenti di Internet possono osservare l'uso del Fast Flux negli attacchi di phishing legati a organizzazioni criminali, incluso l'attacco a MySpace. Vi sono due tipi di fast flux:

- **Single:** è il tipo più semplice di attacco e tali nodi registrano e cancellano il proprio indirizzo come parte della lista degli indirizzi DNS per un singolo dominio. Questo sistema potrebbe essere unito a *round robin DNS* con valori bassi di TTL per creare una lista di indirizzi per un dominio che sarà in continuo cambiamento.
- **Double:** variante più sofisticata rispetto alla precedente in cui nodi registrano e de-registrano il proprio indirizzo come parte della lista dei record NS per una certa zona.

Durante un attacco malware, il record DNS punterà ad un sistema compromesso che agirà da proxy. Questo metodo previene il funzionamento di alcuni dei meccanismi tradizionali di difesa, ad es. le ACL. Il metodo può anche mascherare i sistemi dell'attaccante, che sfrutteranno la rete attraverso una serie di proxy e renderanno più arduo identificare la rete dell'attaccante. Il record normalmente punterà ad un indirizzo IP dove i bot vanno per registrarsi, per ricevere istruzioni o per attivare degli attacchi. Siccome gli IP passano attraverso un proxy, è possibile contraffare l'origine di queste istruzioni, aumentando la possibilità di superare le ACL IP che sono state messe nella rete.

4. Infiltrarsi in una Botnet

Per anni l'attività delle Botnet era motivata principalmente da rancori e danni. Bot Botmaster rivali potrebbero tentare di assoggettarsi l'un l'altro sommergendo l'altrui centro di Comando e Controllo con traffico Bot.

Essendo le Botnet uno strumento di guadagno sempre più in via di diffusione un hacker che non fosse capace di costruire un Bot, potrebbe cercare di infiltrarsi in una rete di Bot già esistente. I metodi di infiltrazione variano a seconda del tipo di canale utilizzato dalla Botnet.

- **IRC**: l'infiltrato si collega al server riuscendo ad avere l'elenco dei Bot che risultano ad esso connessi ed essendo quindi in grado di . Essendo un Bot a tutti gli effetti l'infiltrato riceve anche tutti i comandi inviati agli altri Bot.
- **Http**: La differenza con l'altro tipo di infiltrazione è che in questo caso i Bot non vengono visti dal computer infiltrato ed inoltre non è in grado di mandarne agli altri host della rete proprio perché l'infiltrato non è direttamente connesso ai Botmaster Server. I comandi potranno essere inviati agli altri soltanto se ci si riuscirà ad infiltrare lato server, vale a dire che l'hacker riesca a farsi riconoscere quale proxy.
- **P2P**: Il Bot che desidera infiltrarsi nella rete si connette tramite il protocollo P2P come se fosse un qualsiasi altro host appartenente alla rete e richiede la chiave, solitamente costituita dall'hash dell'indirizzo IP del nodo. Una volta che l'hacker si è riuscito a connettere, riuscirà a vedere tutti i comandi inviati agli altri Bot. Nel caso in cui questi riesca addirittura ad elevarsi a proxy assumerà nuovi poteri, quali accettare connessioni da parte di altri utenti oppure potrà enumerare e identificare i Bot ad esso connessi. Ovviamente nel caso in cui ci si riesca ad infiltrare a livello di proxy si riusciranno anche ad inviare comandi agli host connessi, si potranno quindi inviare comandi a tali Bot.

5. Le Botnet più famose

Il numero di Botnet negli ultimi anni è andato sempre più crescendo, a partire da quelle che si estendono per poche decine di computer infetti a quelle che riescono ad infettare anche miliardi di PC contemporaneamente. Delle migliaia di Botnet che esistono prenderemo in considerazione solo quelle la cui numerosità di infezioni. Una particolare attenzione verrà posta sul fatto che alcune Botnet riescono ad assoggettare anche sistemi ritenuti finora sicuri, quali potrebbero essere Linux e Mac OSX. Le reti che prendiamo in esame sono:

1. Conflicker
2. Storm
3. Psibot
4. Osx.Iservice

5.1 Conflicker

Tale rete è anche conosciuta col nome di Downup, Downadup e Kido ed è stata identificata per la prima volta solo nel 2008. Il Bot sfrutta principalmente l'exploit dell'aggiornamento Microsoft MS08-67 che permette l'esecuzione di RPC anche da parte di utenti che non possiedono le autorizzazioni necessarie. È stato difficile contrastare tale attacco a causa delle diverse tecniche malware che tale exploit permette di sfruttare e che sono utilizzate dal worm. È stata sicuramente considerata l'infezione che si è estesa maggiormente nel 2003. Questo worm ha la capacità di aggiornarsi automaticamente e di migliorarsi in maniera trasparente all'utente evolvendosi in ben 5 varianti diverse con potenzialità sempre maggiori:

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.

5.2 Storm

Questa rete è sicuramente la più famosa e vasta in assoluto, infatti, grazie al Worm Storm inviato tramite email di spam, sono riusciti a compromettere oltre un milione di PC in brevissimo tempo. Le capacità di contaminazione di questa rete variano dai 6.000 host già compromessi che hanno solo il compito di diffondere il worm e offerta del download di musica gratuita da parte di siti che hanno come reale scopo quello di infettare gli altri host. Tale rete possiede anche tecniche di auto protezione, che consistono la protezione dei C&C server tramite tecniche di fast flux su DNS e di una ripetuta codifica del Worm da parte dell'Botmaster. La contaminazione di un host avviene attraverso l'esecuzione sequenziale di alcun i programmi su tale macchina, ciascuno con scopi diversi:

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

5.3 Psib0t

Nonostante la maggior parte dei Bot riesca a sfruttare le falle presenti in molti sistemi Windows ce ne sono alcuni che tendono ad attaccare bug presenti in sistemi Unix based come può essere linux o Mac OSX. Prendiamo in considerazione due Botnet che si sono contraddistinte per aver attaccato proprio questi sistemi solitamente considerati sicuri. Il primo worm che prendiamo in considerazione è sicuramente quello che attacca i router che hanno un sistema operativo Linux. Il worm destinato ad attaccare tali router aveva a disposizione una base di dati con all'interno oltre 6000 username e 13000 password che serviranno al Bot per eludere le difese di tali router. L'attacco prevede, dopo la localizzazione del router vulnerabile, l'uso del

comando telnet per connettersi ad esso. Nel caso si riesca ad individuare la password di root per tale router si eseguirà il download del codice malevolo tramite il comando *wget.* Terminato il download di tale programma questo verrà eseguito per:

- Impedire che vengano effettuate altre connessioni al router che si sta infettando utilizzando nuovamente il comando telnet.
- Si stabilisce una connessione con un server IRC.
- Si associa il PC infettato ad un canale IRC facendo in modo che questo possa ricevere i comandi del Botmaster.

Anche i router, come se fossero dei normali host, dopo la lo contaminazione eseguono una scansione della rete per cercare altri route da infettare e quindi da far entrare nella Botnet.

5.4 Osx.Iservice

Questo programma ha la capacità di attaccare sistemi che montano MAC OSX e si diffonde attraverso la rete P2P. Prende infatti piede attraverso lo scaricamento di software pirata ed ha l'effetto di carpire la password di accesso e di assumere che poi il controllo dei sistemi che lo hanno installato. Inizialmente si diffondeva tra gli utenti che scaricavano copie illagli di iWork '09 o Adobe Photoshop CS4 le cui versioni venivano modificate per installare in aggiunta anche il codice maligno del suddetto Bot. Questo esempio assume un valore particolare poiché è considerato il primo tentativo di creazione di una Botnet di computer MAC che sia mai andato a buon fine.

6. Difendersi dalle Botnet

Abbiamo sinora visto i danni che una Botnet può causare alla rete ed ai singoli utenti. Ciascun utente può però adottare delle contromisure utili sia a rendere più difficile la penetrazione dell'host che a combatterla una volta che sia in atto. Le azioni che possono essere intraprese possono raggiungere tre diversi 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.

Per quanto riguarda le misure di prevenzione che possono essere adottate dall'utente affinché il suo sistema non venga contaminato sono:

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

Vi sono alcuni comportamenti anomali che possono insospettire l'utente e di cui si dovrebbe tener conto. Più in particolare bisognerebbe:

1. Notare una quantità insolitamente alta di traffico sulla porta 6667.
2. Verificare un eccessivo ritardo nelle risposte da parte della rete.
3. Ricevere grandi volumi di traffico su porte insolite.
4. Identificare dei tipi di Bot conosciuti dall'antivirus.

5. Utilizzare risorse online che ispezionino il sistema.

Infine ci sono delle azioni che potrebbero essere fatte una volta che ci si sia accertati che purtroppo il computer fa parte di una Botnet e sono:

- 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.

Infine ci sono delle azioni che lo stesso amministratore può intraprendere per evitare che il suo sistema venga contaminato:

- 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.

Bibliografia

[1] Elizabeth Van Ruitenbeek, William H. Sanders: Modeling Peer-to-Peer Botnets. QEST 2008: 307-316. http://www.perform.csl.illinois.edu/Papers/USAN_papers/08VAN02.pdf

[2] Robert F. Erbacher, Adele Cutler, Pranab Banerjee, Jim Marshall: A Multi-Layered Approach to Botnet Detection. Security and Management 2008: 301-308. http://digital.cs.usu.edu/~erbacher/publications/BotNetArchitecture2.pdf

[3] Moheeb Abu Rajab Jay Zarfoss Fabian Monrose Andreas Terzis: A Multifaceted Approach to Understanding the Botnet Phenomenon. Proceedings of ACM SIGCOMM/USENIX Internet Measurement Conference (IMC), Oct. 2006. Rio de Janeiro, Brazil. http://conferences.sigcomm.org/imc/2006/papers/p4-rajab.pdf

[4] Ramneek Puri: Bots & Botnet: An Overview. August 08, 2003 GSEC Practical Assignment Version 1.4b Option 1 – Research on Topics in Information Security. http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299

[5] David Dittrich, Sven Dietrich: Discovery techniques for P2P botnets. Stevens CS Technical Report 2008-4, September 2008. Revised April 2009. http://www.cs.stevens.edu/~spock/pubs/dd2008tr4.pdf

[6] Thorsten Holz, Moritz Steiner, Frederic Dahl, Ernst W. Biersack, and Felix Freiling: Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. In First Usenix Workshop on Large-scale Exploits and Emergent Threats (LEET), San Francisco, CA, USA, April 2008. http://honeyblog.org/junkyard/presentations/08_storm_LEET.pdf

[7] Ben Stock, Jan Gobel, Markus Engelberth, Felix C. Freiling, and Thorsten Holz: Walowdac Analysis of a Peer-to-Peer Botnet. Computer Network Defense (EC2ND), 2009 European Conference on 9-10 Nov. 2009. http://pi1.informatik.uni-mannheim.de/filepool/publications/waledac-paper.pdf

[8] John Syers: State of the art botnet-centric Honeynet design. JOHN SYERS III'S THESIS for Texas A&M University for the degree of Master of Computer Science. May 2009. http://repository.tamu.edu/bitstream/handle/1969.1/ETD-TAMU-2009-05-666/Syers.pdf?sequence=2

[9] Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski,Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna: Your Botnet is My Botnet: Analysis of a Botnet Takeover. In the Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 2009 November 9-13, 2009, Chicago, IL, USA. http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf

[10] Martin Overton: Bots and Botnets: Risks, Issues and Prevention. Virus Bulletin Conference 5/10/2005. http://www.virusbtn.com/pdf/conference_slides/2005/MO-VB2005.pdf

[11] Jun-Yi Zheng: Botnet Detection by Monitoring Group Activities in DNS Traffic. Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on: 715 – 720. http://mmnet.iis.sinica.edu.tw/botnet/file/20091123/20091123_1.pdf

[12] Ping Wang, Sparks, S. ; Zou, C.C. : An Advanced Hybrid Peer-to-Peer Botnet. Dependable and Secure Computing, IEEE Transactions on : 113 – 127. http://www.usenix.org/event/hotbots07/tech/full_papers/wang/wang.pdf

[13]John C. A. Bambenek: Botnets: Proactive System Defense. Urbana-Champaign. SpringerLink chapter of "Botnet Detection. Countering the largest security threat" by Wenke Lee, Cliff Wang and David Dagon. Springer 2007. http://www.springerlink.com/content/978-0-387-68766-7/#section=190719&page=3&locus=68

[14]Jason Franklin, Vern Paxson: Understanding Botnets: How Massive Internet Break-Ins Fuel an Underground Economy. Poster session, Lawrence Berkeley National Laboratory, Berkeley, CA, July 2006. http://www.cs.cmu.edu/~jfrankli/talks/botnet_underground_economics.ppt

[15] David Dagon, Cliff Changun Zou, Wenke Lee: Modeling Botnet Propagation Using Time Zones. In Proceedings of the 13 th Network and Distributed System Security Symposium NDSS. http://www.isoc.org/isoc/conferences/ndss/06/proceedings/papers/modeling_botnet_propagation.pdf

[16]Tyler Moore, Richard Clayton, and Ross Anderson: The Economics of Online Crime. Journal of Economic Perspectives—Volume 23, Number 3—Summer 2009: 3 – 20. http://people.seas.harvard.edu/~tmoore/jep09.pdf

[17]Hossein Rouhani Zeidanloo, Azizah Abdul Manaf: Botnet Command and Control Mechanisms. 2009 Second International Conference on Computer and Electrical Engineering. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5380180

[18]Feily, M., Shahrestani, A., Ramadass, S.: A Survey of Botnet and Botnet Detection. Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on : 268 – 273. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5210988

[19]Symantec 2008: Symatec Global Internet Security Threat Report, Vol. 13, Trends for July–December 07.

[20] Panda Security 2009: More than 10 Million Worldwide Were Actively Exposed to Identity Theft in 2008. March 10.

[21]Moore, Tyler, and Richard Clayton. 2009: Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing. Lecture Notes in Computer Science, vol. 5628. 256–72.

[22]Provos, Niels, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose 2008: All Your iFRAMEs Point to Us. Proceedings of the 17th USENIX Security Symposium, 1–15. USENIX Association.

[23]APACS (Association for Payment Clearing Services) 2008: APACS Announces Latest Fraud Figures. Press release, September 25.

[24]Gartner. 2006: Gartner Says Number of Phishing E-Mails Sent to U.S. Adults Nearly Doubles in Just Two Years. Press release, November 9.

[25]Computer Economics. 2007: Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and other Malicious Code.

[26] http://it.wikipedia.org/wiki/Botnet

[27] http://en.wikipedia.org/wiki/Botnet

[28] http://en.wikipedia.org/wiki/DoS

[29]http://en.wikipedia.org/wiki/Adware

[30]http://en.wikipedia.org/wiki/Spyware

[31]http://en.wikipedia.org/wiki/Email_spam

[32]http://it.norton.com/theme.jsp?themeid=botnet

[33]http://www.geekissimo.com/2009/09/15/linux-scovata-una-botnet-che-inietta-malware-a-destra-e-a-manca/ (Pagina web che tratta della scoperta di Botnet che coinvolgono anche computer con sistema operativo Unix.)

[34]Kelly Jackson Higgins: The World's Biggest Botnets. 11/2007. http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208808174 (Articolo che fa un breve panoramica delle Botnet più famose che hanno attaccato il web, in particolare su Storm.)

[35]Davey Winder: Battle of the botnets. May 2007. http://www.daniweb.com/news/story218515.html (Articolo che si occupa principalmente di fare una breve descrizione della guerra che i vari Botmaster ingaggiano contro altre Botnet.)

[36]Vitaly Kamluk: The botnet business. 1997-2010 Kaspersky Lab http://www.securelist.com/en/analysis/204792003/The_botnet_business

[37]Zeljka Zorz: The botnet economy. 04/2010. http://www.net-security.org/secworld.php?id=9121 (Articolo che spiega i vantaggi economici che i Botmaster possono trarre dalle loro Botnet.)

[38]Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng, Jingyuan Zhang: Botnet: Classification, Attacks, Detection, Tracing and Preventing Measures. http://www.hindawi.com/journals/wcn/2009/692654.html. EURASIP Journal on Wireless Communications and Networking Volume 2009 (2009), Article ID 692654, 11 pages. (Panoramica dettagliata sulle Botnet con particolare attenzione ai tipi di attacchi che possono essere portati.)

[39]http://www.honeynet.org/node/53 (Sito di Honeynet Project in cui si trova la descrizione delle varie famiglie a cui i Bot potrebbero appartenere.)