1. Definição de bot
2. Protocolos usados - IRC
3. Como se propaga – atacante e vítima , prioridade de contaminação
4. Botnet – Definição
5. Topologias de comunicação da botnet
6. Atividades maliciosas
7. Defesa : prevenir, detectar e responder
8. Botnets Legais

1)

O termo bot é derivado de “*robot*” (robô em inglês). Bot é um termo genérico usado para descrever um script ou um conjunto de scripts criados para desempenhar funções preestabelecidadas de forma automatizada. Bots são utilizados por máquinas de buscas para caminhar pela *web* tomando conhecimento dos conteúdos dos *websites* e em jogos onlines para prover oponentes virtuais. Como exemplo concreto podemos citar a rede IRC na qual as funções dos bots nos canais incluem acesso à listas, movimentação de arquivos, compartilhamento de usuários , compartilhamento de informação do canal, e muitas outras funcionalidades desde que os devidos *scripts* sejam adicionados corretamente [11].

2)

Diversos protocolos podem ser utilizados para a realização de comunicação em botnets. Dentre os mais conhecidos temos o *Internet Relay Chat* (IRC).  
O IRC é um protocolo de *internet* criado pelo finlandês Jarkko Oikarinen, em 1998. O objetivo desse protocolo é permitir que as pessoas conectadas à *internet* possam interagir em conversas por texto em tempo real [11]. Cada discussão está em um canal e várias pessoas podem ingressar nesse canal conjuntamente. O protocolo IRC é baseado na arquitetura cliente-servidor , e é apropriada para execução distribuída em várias máquinas.

3)

Os bots podem ser utilizados de forma maliciosa. Isto ocorre através da infecção de máquinas (vítimas) por meio do atacante através da exploração de vulnerabilidades, de aplicações ou do próprio sistema operacional, ou instalação do bot de forma não intencional. Após ser instalado o bot modifica variáveis do sistemas operacional para que seja inicializado toda vez que o sistema for inicializado. Com isso, os bots das máquinas vítimas (bots agentes) estariam conectados com o bot da máquina atacante, a esse bot damos o nome de bot mestre. Alguns parâmetros podem ser utilizados para o estabelecimento de prioridades de contaminação de máquinas em meio ao universo de possíveis alvos. Dentre esses parâmetros temos a quantidade de banda disponível por meio desse bot, poder de processamento dessa máquina,etc. O bot mestre pode causar grandes danos ao utilizar conjuntamente os bots presentes nas máquinas infectadas, as atividades maliciosas que podem ser realizadas serão melhor detalhadas na seção 6.

4)

Um conjunto de bots agentes servindo juntos a um mesmo bot mestre constitui uma botnet. Com a finalidade de possibilitar a interação entre os bots e o bot mestre foram criadas algumas capacidades de comunicação que possibilitariam a recepção de comandos e o envio de resultados ao bot mestre. Segundo [6], existem dois tipos diferentes nos quais um bot pode receber comandos de seu mestre, são eles: (1) o modo de “puxar” e o modo de “empurrar”. Ambos precisam de um servidor de *command-and-control* (C&C) que “conversa” com os bots agentes.

5)

Diversas topologias C&C são empregadas com o intuito de garantir defesas comerciais, desligamentos determinados por lei e tentativas de “sequestro” de bots [15]. Essas topologias vem sendo otimizadas para reduzir *network chatter* e a as falhas do sistema. As principais topologias utilizadas são : estrela, multi-servidor, hierárquica e randômica.

A topologia estrela possui um único centralizado recurso de C&C para se comunicar com todos os demais bots. Cada bot recebe instruções diretamente do ponto central C&C [15].

|  |  |
| --- | --- |
| Vantagem | Desvantagem |
| A comunicação direta entre o C&C e o bot agente possibilita a transferência de instruções (e dados roubados) rapidamente [15]. | Possui um ponto único de falha. Caso o C&C central for bloqueado ou desabilitado, toda a botnet é neutralizada [15]. |





A topologia de C&C multi-servidor é uma extensão lógica da topologia estrela, na qual vários servidores são utilizados para prover instruções de C&C para os bots agentes[15]. Esses servidores comunicam entre si enquanto gerenciam a botnet. Essa topologia de C&C é mais refinada e por isso exige uma maior esforço para ser implementada, porém por ter seu C&C descentralizado torna-se possível a manutenção da botnet mesmo caso um dos servidores de C&C forem derrubados.





|  |  |
| --- | --- |
| Vantagens | Desvantagem |
| Não possui um ponto único de falha. Caso um dos servidores C&C forem bloqueados ou desabilitados os remainescentes ainda são capazes de manter o controle de todos os demais bots agentes da botnet. | Exige mais esforço e conhecimento para a construção da infraestrutura de um C&C multi-servidor. |
| Torna possível a realização de otimizações geográficas por meio da distribuição adequada dos servidores de C&C aumentando a velocidade da comunicação entre os elementos da botnet. |  |

A topologia hierárquica reflete a dinâmica dos métodos utilizados na contaminação e na posterior propagação dos bots. Os bots agentes tem a habilidade de transmitir novas instruções de C&C para bots agentes propagados anteriormente. A utilização desse método de propagação geralmente gera problemas com latência tornando difícil para o operador da botnet utilizar a botnet para atividades de tempo real [15].

Nessa topologia nenhum bot tem conhecimento da localização da botnet como um todo. Essa característica dificulta a determinação o tamanho de uma botnet. Essa estrutura também favorece a escalabilidade da botnet.

|  |  |
| --- | --- |
| Vantagens | Desvantagem |
| A interceptação ou tomada de controle dos bots agentes não enumerará todos os membros da botnet nem o servidor de C&C. | Devido a necessidade de transmissão de comandos por meio de múltiplos canais de comunicação há latência. |
| Maior escalabilidade da botnet. |  |

A topologia randômica não possui uma estrutura de C&C centralizada. Os comandos são introduzidos na botnet por meio de qualquer bot agente. Esses comandos geralmente fazem com que o bot agente propague automaticamente os comandos para todos os demais bots agentes presentes na botnet [15] .

|  |  |
| --- | --- |
| Vantagem | Desvantagens |
| A ausência de uma infraestrutura de C&C centralizada e o modelo de comunicação empregado torna muito dificil de derrubar a botnet. | A latência gerada pela natureza randômica dos *links* utilizados para a realização da comunicação de C&C. |
|  | É possível a identificação de bots agentes por meio do monitoramento das comunicações de um dado bot agente. |

6)

Diversas atividades maliciosas podem ser desempenhadas com o uso de botnets. A principal é o ataque por negação de serviços distribuidos (DDoS, em inglês), cujas informações se encontram na seção dedicada a ele. Atividades como a “infecção local secundária” ( secondary local infection) forçando a instalação de key logger ou trojan para a obtenção de dados pessoais da vítima [11] . Demais atividades como “troca de banda”, *backdoor* e armazenamento de dados ilegais também serão abordados ao longo desta seção.

7)

* Prevenir
* Detectar
* Responder

8)

* The Honeynet Project
* Charity Engine
* Folding@Home(Stanford)