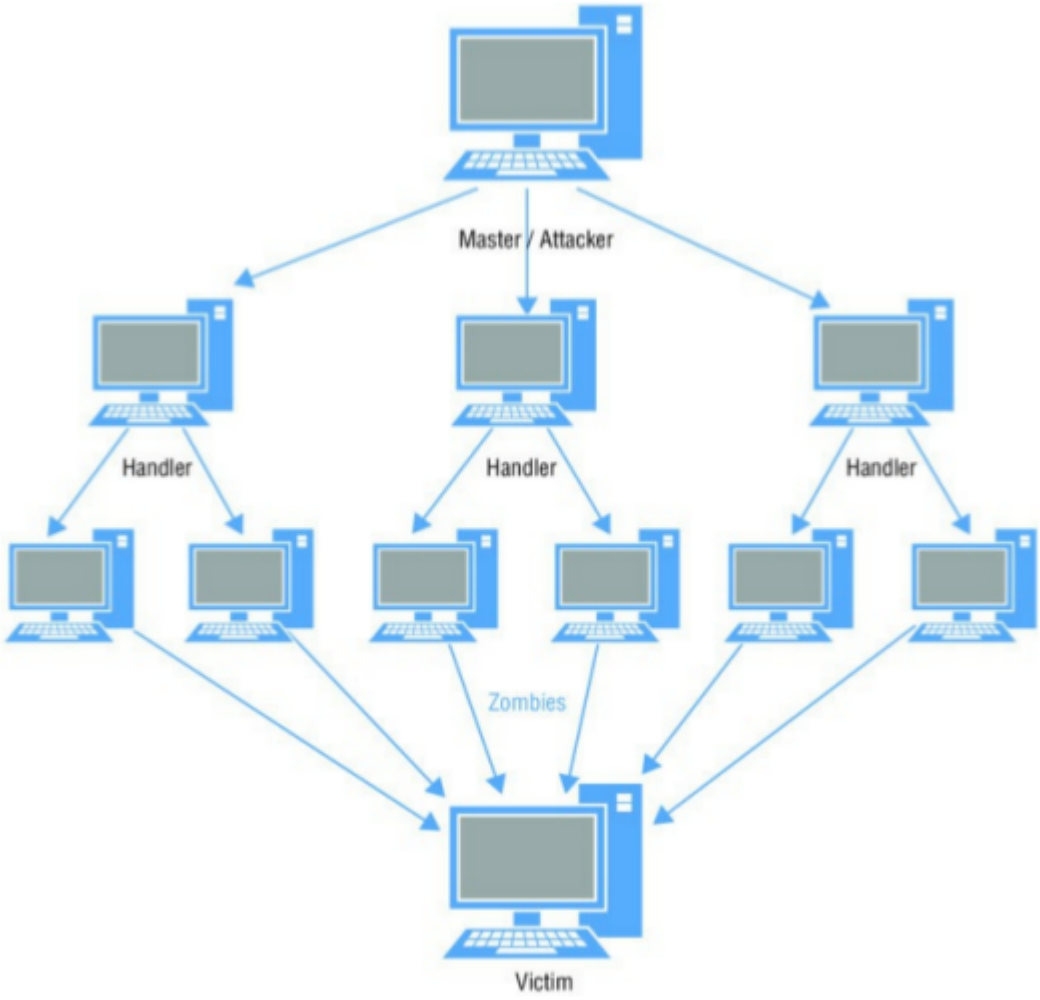
Ataques Distribuídos de Negação de Serviço (DDoS), ferramentas e como se proteger

Os ataques distribuídos de negação de serviço (DDoS) têm os mesmos objetivos do DoS, mas a implementação é muito mais complexa e possui mais poder. Considerando que um ataque DoS depende de um único sistema ou um número muito pequeno de sistemas para atacar uma vítima, um ataque DDoS aumenta a escala por ter vários atacantes indo atrás de uma vítima. Quantos atacantes? Em qualquer valor de algumas centenas a alguns milhões em alguns casos.

Ataques DDoS

Os ataques DDoS têm o mesmo objetivo que os métodos DoS regulares; No entanto, a diferença reside na implementação do ataque. Um ataque DoS padrão pode ser iniciado a partir de um único cliente mal-intencionado, enquanto que um ataque DDoS usa um grupo distribuído de computadores para atacar um único destino. Confira a Figura 11.3 para ver um diagrama de uma configuração de DDoS.



Como você pode ver, algumas partes estão envolvidas ao realizar um ataque DDoS. Conceitualmente, o processo é bastante simples. O atacante primeiro infecta o manipulador, computador master, com uma compilação de software específico DDoS conhecido como um bot. O bot por sua vez se espalha através da rede da vítima à procura de potenciais clientes para torna-los escravos ou zumbis. Observe que o atacante escolhe propositadamente suas unidades baseado na vantagem do posicionamento que lhes dará para seu ataque DDoS. Isso equivale a manobrabilidade na rede que ele tem, como um servidor de arquivos ou semelhante. Uma vez que os sistemas de manipuladores foram comprometidos e os clientes zumbis estão infectados e ouvindo, o atacante precisa apenas identificar o alvo e enviar o sinal de “atacar” para os manipuladores.

Um método comum de instalar secretamente um bot em um manipulador ou cliente é um cavalo de Tróia que carrega o bot

como um payload (carga). Uma vez que o manipulador e os zumbis subsequentes foram infectados, o atacante se comunica remotamente com a chamada botnet via canais de comunicação como o Internet Relay Chat (IRC) ou Peer-to-Peer (P2P).

Ferramentas para criação de Botnets

Várias ferramentas são usadas para criar botnets, incluindo o seguinte:

- Shark
- PlugBot
- Poison Ivy
- Low Orbit Ion Cannon (LOIC)

Ferramentas DoS

Segue uma lista de ferramentas DoS:

- **DoSHTTP** é uma ferramenta de inundação HTTP para DoS. Ele pode segmentar URLs e usa a designação de porta.
- **UDPFlood** ele gera pacotes UDP em uma taxa especificada e para uma rede específica.
- **Jolt2** é uma ferramenta DoS de fragmentação de pacotes IP que pode enviar um grande número de pacotes fragmentados para um host Windows.
- **Targa** é uma ferramenta oito-em-um que pode executar ataques DoS usando uma ou várias das opções incluídas. Ataques podem ser do tipo Land, WinNuke, e teardrop.

Ferramentas DDoS

- **Trinoo** é uma ferramenta DDoS que usa inundação UDP. Pode atacar IPs únicos ou múltiplos.
- O **Low Orbit Ion Cannon (LOIC)** tornou-se popular devido à sua fácil operação com um botão. Algumas pessoas suspeitam que grupos como o Anonymous, que usam ataques

DDoS como sua arma principal, usam o LOIC como sua principal ferramenta.

- **TFN2K** é uma ferramenta de ataque DDoS baseada em TFN (Tribe Flood Network) e pode executar ataques de inundação UDP, SYN e UDP.
- **Stacheldraht** é uma ferramenta DDoS que tem recursos de ataque semelhantes ao TFN2K. Os ataques podem ser configurados para serem executados por um período especificado e para portas específicas.

Estratégias defensivas

Vejamos algumas estratégias defensivas de DoS:

Desabilitando Serviços Desnecessários poderá ajudar a proteger contra ataques de DoS e DDoS em sistemas individuais e implementando medidas de rede que protegem contra tais ataques.

Usando o **Anti-malware** a proteção contra vírus em tempo real pode ajudar a evitar instalações de bot, reduzindo as infecções de Trojan com payloads úteis de bot. Isso tem o efeito de parar a criação de bots para uso em uma botnet. Embora não seja uma defesa contra um ataque real, pode ser uma medida preventiva.

Ativando o Router Throttling Os ataques DoS que dependem da saturação do tráfego da rede podem ser frustrados ou, pelo menos, mitigados, permitindo a limitação de roteamento em seu roteador de gateway. Isso estabelece um controle automático sobre o impacto que um potencial ataque DoS pode causar e fornece um buffer de tempo para que os administradores de rede respondam adequadamente.

Um proxy reverso é o oposto de um proxy direto ou padrão. O recurso de destino, em vez do solicitante, desencadeia o redirecionamento de tráfego. Por exemplo, quando uma solicitação é feita para um servidor da Web, o tráfego

solicitante é redirecionado para o proxy reverso antes de ser encaminhado para o servidor real. O benefício de enviar todo o tráfego para um intermediário é que o intermediário pode tomar uma ação protetora se ocorrer um ataque.

Ativando o filtro de entrada e saída evita ataques de DoS e DDoS filtrando itens como endereços IP falsificados que vêm de fora da rede. Em outras palavras, se o tráfego vindo do lado público de sua conexão tiver um endereço de origem correspondente ao seu esquema de IP interno, então você sabe que é um endereço falsificado. A filtragem de saída ajuda a prevenir ataques DDoS filtrando o tráfego de saída que pode impedir que o tráfego malicioso volte para o atacante.

Serviços degradantes Nesta abordagem, os serviços podem ser automaticamente atenuados ou encerrado em caso de ataque. A ideia é que os serviços degradados tornam o ataque mais difícil e tornam o alvo menos atraente.

Absorvendo o Ataque Outra solução possível é adicionar serviços extras e poder na forma de largura de banda e outro significa ter mais poder do que o atacante pode consumir. Este tipo de defesa exige um monte de planejamento extra, recursos e, claro, dinheiro. Esta abordagem pode incluir o uso de tecnologias de balanceamento de carga ou estratégias semelhantes.

Defesas específicas de Botnet

As estratégias defensivas específicas a botnet são as seguintes:

- **Filtragem RFC 3704** Esta defesa é projetada para bloquear ou parar pacotes de endereços que não são utilizados ou reservados em qualquer intervalo de IP. Idealmente, essa filtragem é feita no ISPlevel antes de alcançar a rede principal.
- **Filtragem Black Hole** Esta técnica, na sua essência, cria

um buraco negro ou área na rede onde o tráfego ofensivo é encaminhado e descartado.

- **Filtragem de reputação do IP de origem** A Cisco oferece um recurso em seus produtos, especificamente suas tecnologias IPS, que filtra o tráfego baseado na reputação. A reputação é determinada pela história passada de ataques e outros fatores.

Sugestões de livros: