1.Ataques Denial of Service

Um ataque de negação de serviço ocorre quando um invasor força um serviço a falhar, tornando-o inacessível para usuários legítimos. Isso pode ser feito sobrecarregando um sistema com solicitações até que ele não consiga mais responder ou explorando vulnerabilidades conhecidas para causar falhas. Manter sistemas sempre atualizados com os patches de segurança mais recentes é fundamental para reduzir o risco desse tipo de ataque. Em alguns casos, organizações mal-intencionadas podem utilizar ataques de negação de serviço contra concorrentes para obter vantagem competitiva. Além disso, esses ataques também podem ser usados como distração para ocultar outras invasões acontecendo simultaneamente.

Embora algumas negações de serviço aconteçam devido a falhas de software, outras podem ser provocadas de maneiras extremamente simples. Desligar a energia de um data center, por exemplo, pode interromper completamente seus serviços. Em certos casos, as empresas podem causar a própria negação de serviço por acidente, como quando um administrador conecta dois switches de rede de forma incorreta, criando um loop que derruba parte da infraestrutura. Outra forma comum de sobrecarga acontece quando um único usuário baixa um arquivo grande, como uma distribuição Linux, consumindo toda a largura de banda disponível e afetando os serviços críticos da rede. Há até situações mais inusitadas, como vazamentos de água dentro de um data center, que podem causar pânico e interromper operações essenciais.

Os atacantes frequentemente não confiam em um único dispositivo para causar grandes impactos. Em vez disso, utilizam múltiplos dispositivos distribuídos globalmente para realizar um **ataque distribuído de negação de serviço (DDoS)**. Esse tipo de ataque sobrecarrega servidores, consumindo sua largura de banda ou recursos computacionais, tornando-os inacessíveis para usuários legítimos. Para isso, os criminosos criam redes de dispositivos infectados, chamadas de **botnets**, que obedecem a comandos centralizados. O botnet Zeus, por exemplo, chegou a controlar mais de 3,6 milhões de computadores em seu auge, permitindo que os invasores direcionassem ataques massivos com apenas um único comando.

Uma das razões pelas quais os ataques DDoS são tão eficazes é que eles representam uma ameaça **assimétrica**. Com poucos recursos, um atacante pode sobrecarregar grandes organizações, que possuem uma infraestrutura muito mais robusta. Além disso, os criminosos descobriram maneiras de amplificar seus ataques, enviando pequenos pacotes de dados que resultam em respostas muito maiores. Isso ocorre explorando serviços de rede comuns, como DNS e NTP, que naturalmente enviam respostas mais volumosas do que as solicitações originais.

O ataque de amplificação DNS é um dos mais utilizados nessa categoria. Para realizá-lo, o invasor instrui seu botnet a enviar consultas DNS para servidores configurados incorretamente, solicitando grandes quantidades de

dados. No entanto, esses pedidos são falsificados, de modo que as respostas não retornam para o atacante, mas sim para o alvo do ataque. Como as respostas são muito maiores que as solicitações iniciais, o alvo rapidamente se sobrecarrega e se torna inacessível.

Esse tipo de ataque demonstra a importância de configurar corretamente servidores DNS e outros serviços de rede para evitar serem explorados como vetores de amplificação. Além disso, empresas e provedores de internet podem implementar mecanismos de mitigação, como filtragem de tráfego suspeito e uso de firewalls avançados para bloquear padrões conhecidos de ataques DDoS. A proteção contra negações de serviço exige uma abordagem proativa, combinando boas práticas de configuração, monitoramento contínuo e soluções especializadas para garantir que serviços críticos permaneçam disponíveis mesmo diante de tentativas de sobrecarga maliciosa.

2.Ataques DoS - Extras

Este ataque impede o uso normal de um computador ou rede por usuários válidos. Após obter acesso a uma rede, um ataque DoS pode travar aplicativos ou serviços de rede. Um ataque de DoS pode inundar um computador ou toda a rede com tráfego até que um desligamento ocorra devido a sobrecarga.