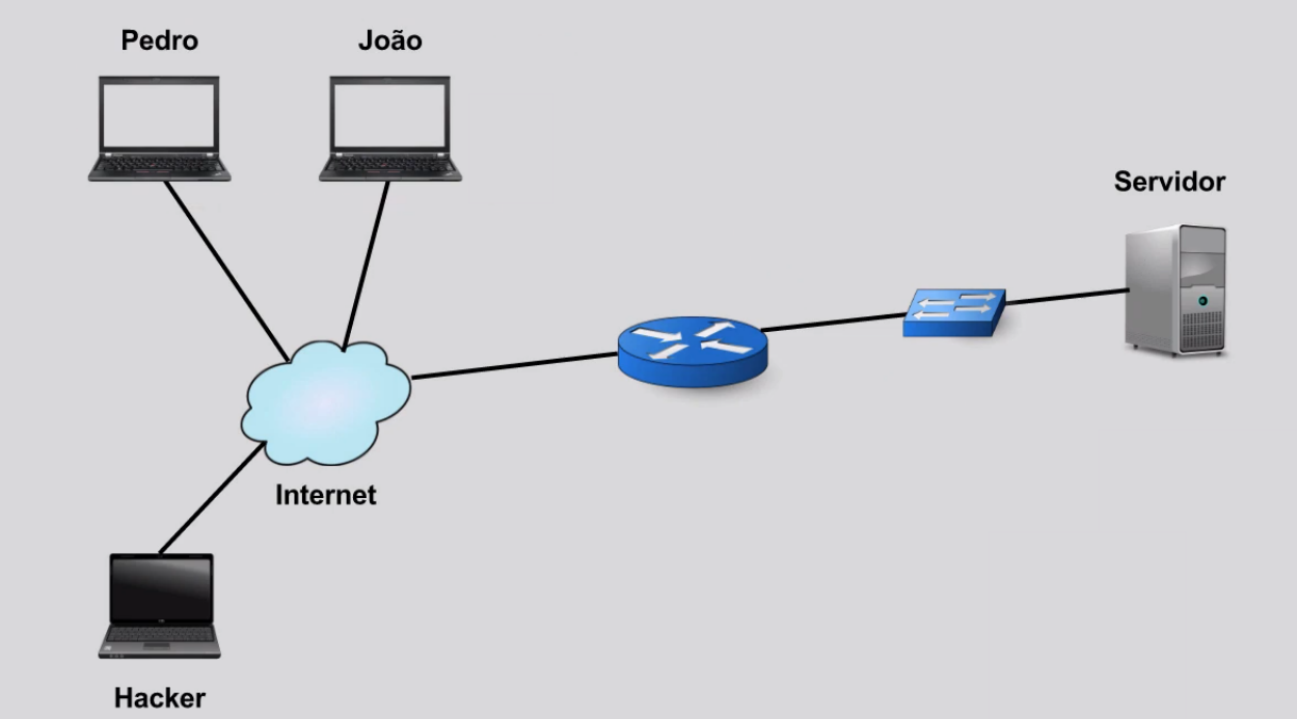
08

Ataques distribuído (Ddos)

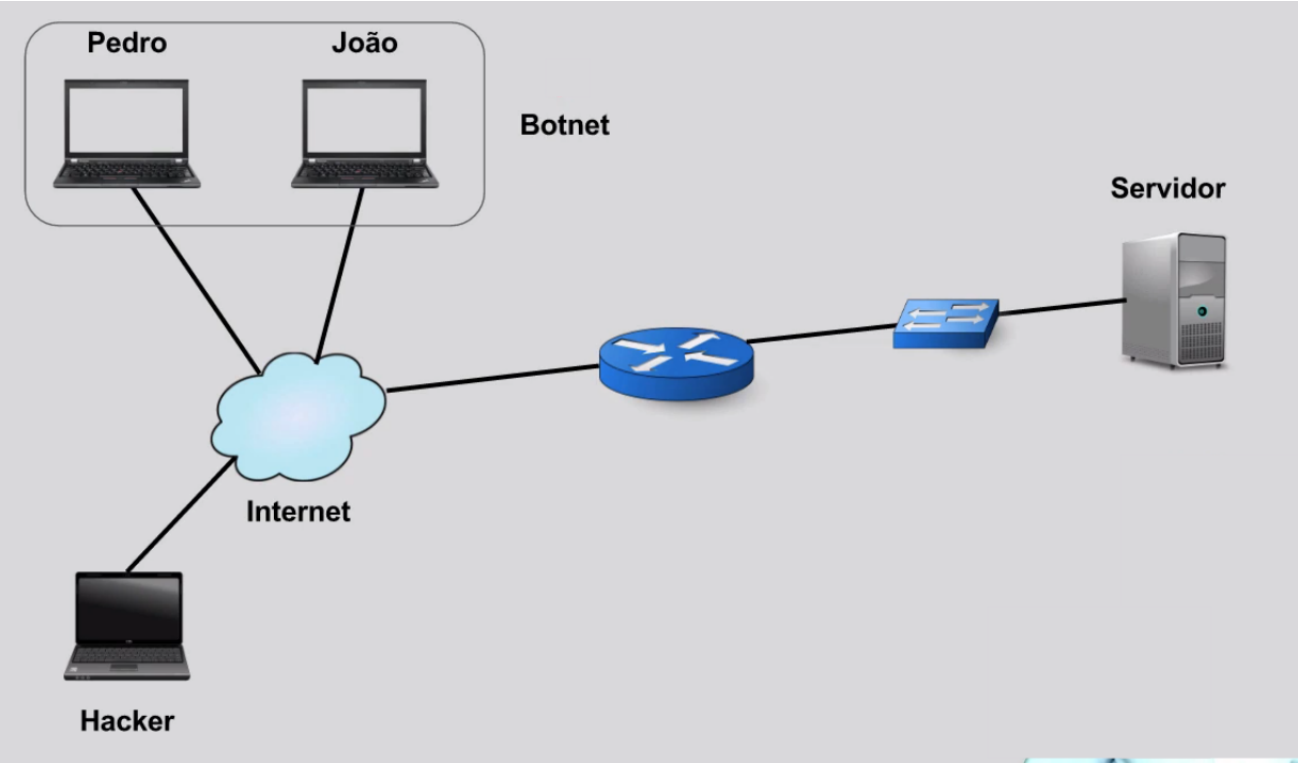
Transcrição

Quando realizamos o ataque com o slowloris, conseguimos comprometer o servidor ao abrir uma série de portas e conexões com ele. Por não haver nenhum equipamento de detectasse ou prevenisse ataques (IDS ou IPS), ele aconteceu facilmente. Com um desses equipamentos, o cenário seria diferente.

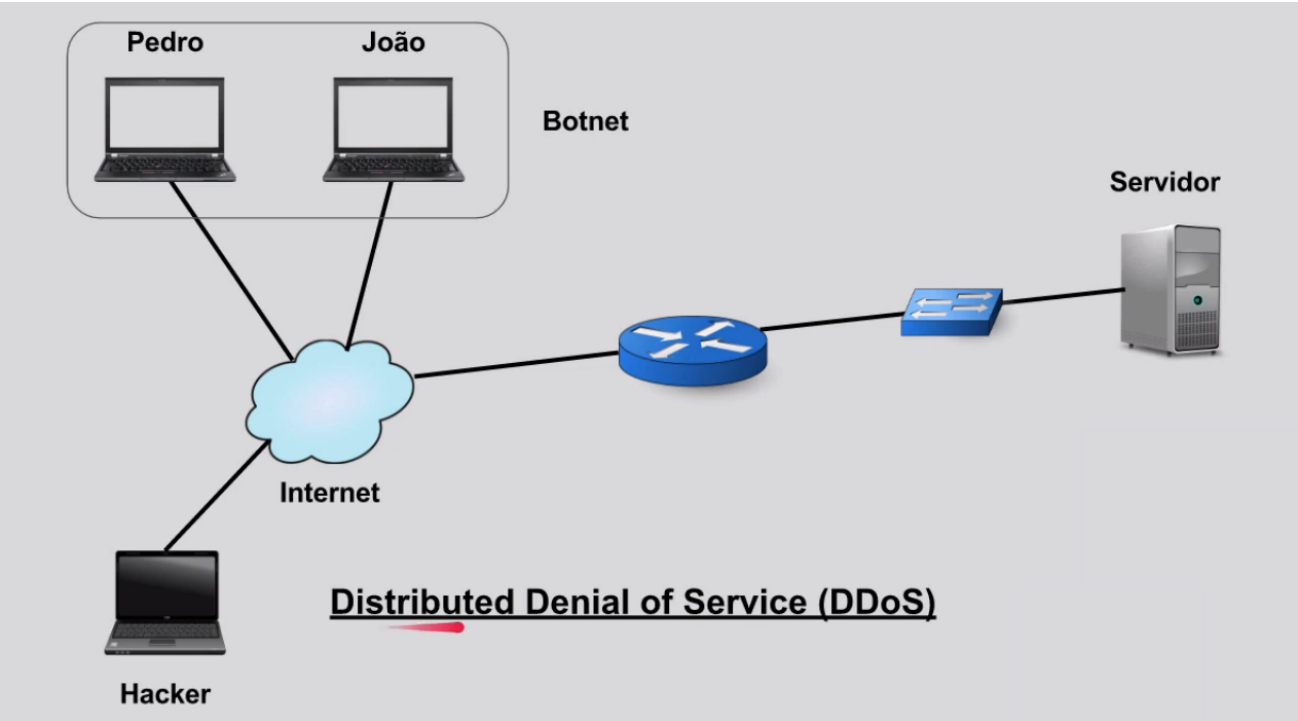
Agora o hacker não vai mais tentar fazer esse ataque sozinho. Ele terá um grupo de pessoas engajado em ajudá-lo. A ideia dele é comprometer o computador de duas vítimas, que chamaremos de Pedro e João, para tentar indisponibilizar o serviço. O ataque estará distribuído em várias máquinas, que estão tentando comprometer o servidor mandando uma grande quantidade de tráfego.



Essas duas máquinas, que comprometemos no intuito de ter ajuda em um ataque, são chamadas de **Botnet**. O hacker faz com que essas máquinas pertençam ao seu exército para auxiliar em seus ataques.



Isso pode ser feito por meio de vírus ou malware, que ao serem recebidos, sequestram as máquinas para o exército do hacker. Por ser distribuído, o ataque é chamado de *Distributed Denial of Service*, ou DDoS. No português ficaria "Ataque de negação de serviço distribuído".



Esse é um dos ataques mais temidos por organizações, não porque o objetivo principal do ataque seja roubar informações ou algo assim, mas por sua difícil detecção. Como o ataque é realizado por várias máquinas em diferentes localidades do mundo, é difícil saber quem está fazendo um acesso legítimo ao site e quem está acessando de maneira indevida. Fica bem complicado de descobrir quais são as máquinas (e os seus IPs) que estão participando do ataque ou acessando o servidor de maneira ilegal.

Por isso, o DDoS não é apenas um dos ataques mais temidos, mas também um dos mais efetivos. Durante a minha pesquisa para montar o curso, encontrei alguns ataques DDoS recentes. Dentre eles, selecionei duas notícias interessantes.

A primeira delas, disponível aqui (http://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/), fala sobre um vírus (*worm*) do malware Mirai que conseguiu derrubar 900 mil pessoas na Alemanha. Acredita-se que o botnet do Mirai gira por volta de 400 mil máquinas. Imagine só o impacto dessa imensa quantidade de máquinas realizando um ataque a um servidor de determinada empresa. É uma quantidade de tráfego muito grande.

A segunda notícia (http://www.ibtimes.co.uk/anonymous-hacktivists-launch-ddos-attacks-against-websites-donald-trump-1552750) fala do grupo Anonymus.

O grupo estava tentando realizar um ataque de DDoS contra os sites de hotéis e outros empreendimentos do presidente dos EUA Donald Trump. Lendo essa reportagem, descobrimos que eles estavam perto de alcançar um terabyte de tráfego nesses servidores. E por causa disso, o link tende a não suportar essa demanda e o link fica indisponível.

Imagine uma situação dessas para empresas como a Amazon, o Facebook e outras com um grande volume de clientes. Eles teriam uma grande perda de receita. É um impacto muito grande, que junto com a dificuldade de identificar quem está efetivamente o realizando, torna os ataques de DDoS muito devastadores e temidos.