DDoS: como funciona um ataque distribuído por negação de serviço

Entenda como aconteceu a queda dos servidores dos sites do governo brasileiro

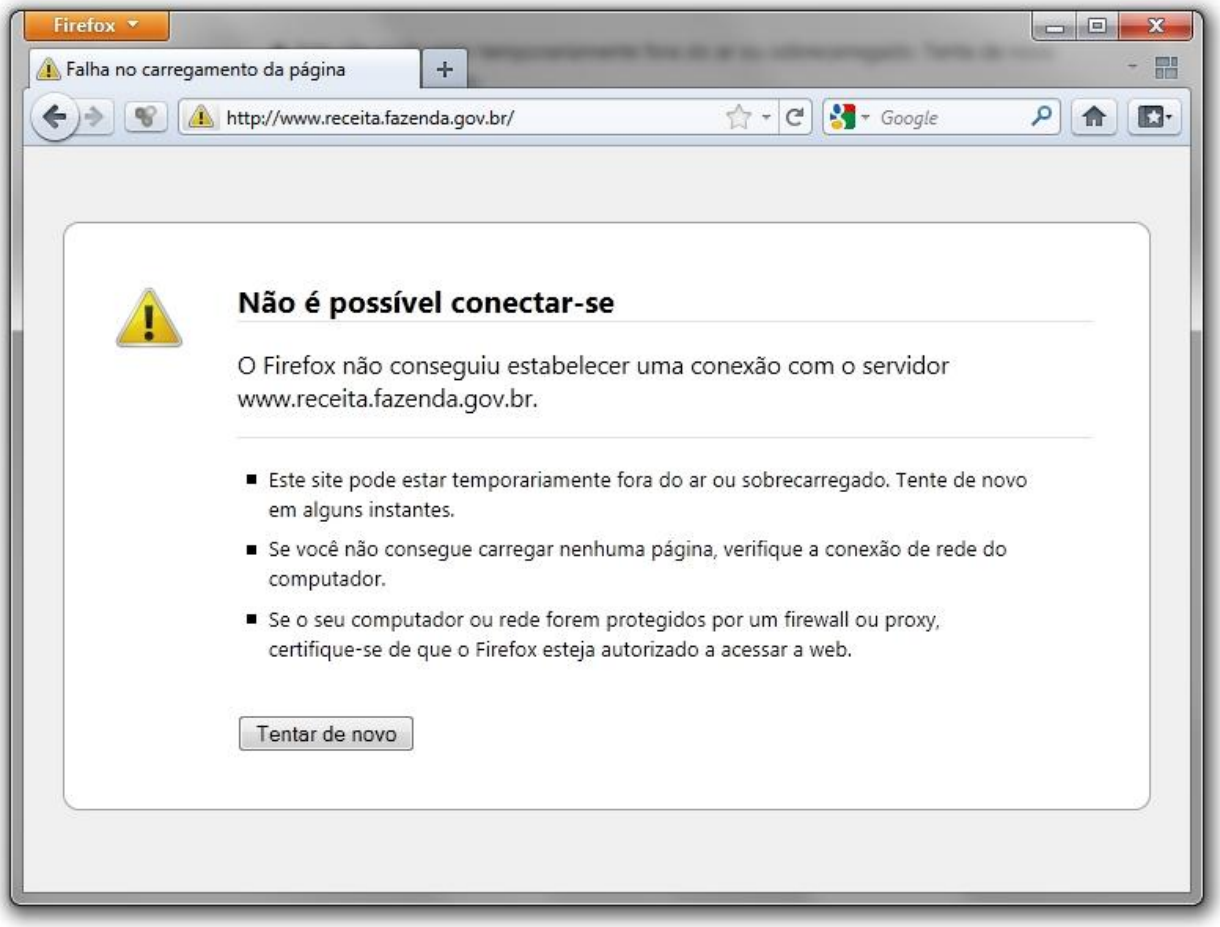
Por Fabio Jordão em 24 de Junho de 2011

Está repercutindo em todos os sites de tecnologia e de notícias. Aconteceram, nessa terça-feira (22), ataques aos sites da Receita Federal, da Presidência da República, do Portal Brasil e da Petrobrás. Você possivelmente já deve saber quem são os responsáveis pelos ataques, porém talvez ainda não faça ideia de como os hackers tiraram do ar os sites do governo brasileiro.

Para esclarecer um pouco esses misteriosos ataques, o Tecmundo vai lhe explicar o tipo utilizado e como ele funciona. Contudo, antes de esclarecermos os pormenores do ataque hacker, vamos falar sobre os servidores da web, que estão diretamente ligados ao assunto.

Por trás de toda página há um servidor

Os sites do governo, assim como quaisquer outros, ficam hospedados em computadores dedicados e de alta capacidade. Essas máquinas são chamadas de servidores e recebem esse nome porque servem às solicitações efetuadas pelos clientes (usuários comuns, como você que está lendo esta matéria).



Assim como qualquer sistema do mundo, os servidores possuem limitações, tanto no processamento de informações quanto no envio e recebimento de dados. As limitações de processamento ocorrem porque essas máquinas possuem processadores que não têm “poder” infinito. Além disso, elas são equipadas com uma determinada quantidade de memória, a qual pode ser esgotada conforme o número de processos em execução.

Já as limitações no envio e recebimento de dados ocorrem porque os servidores são equipados com placas de rede, as quais possuem especificações que determinam o máximo de dados que podem trafegar. Isso significa que um servidor não pode enviar dados infinitos e nem mesmo com velocidade capaz de atender ao máximo que um cliente requisita. Além disso, o sistema que gerencia o servidor possui uma limitação de slots (requisições), o que determina o máximo de usuários que podem ser atendidos simultaneamente.

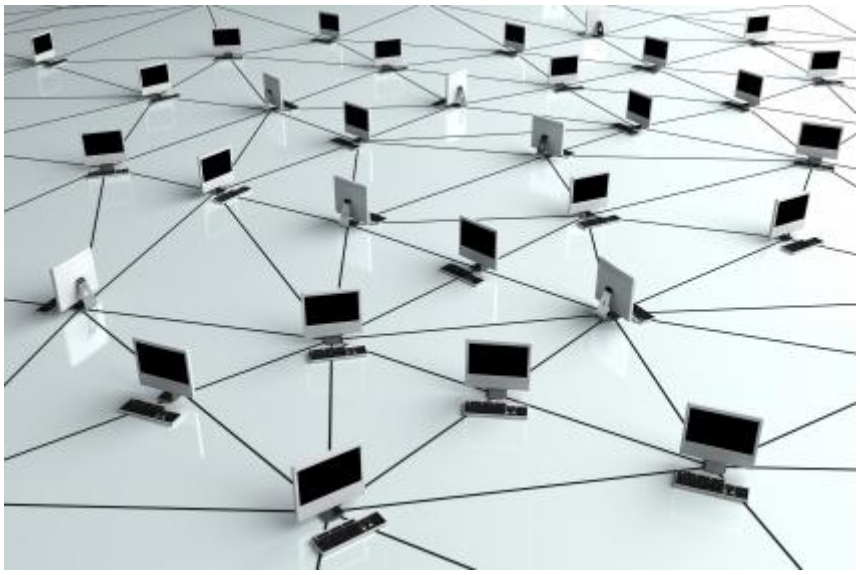
Vale salientar que essa explicação é apenas um esboço do todo que acontece por trás de um site da web. Na realidade, uma página grande da internet tem múltiplos servidores, os quais conseguem atender milhares ou milhões de clientes (usuários) simultaneamente.

Excedendo os limites

Um ataque hacker pode acontecer de diversas maneiras e ter diferentes objetivos. O tipo de ataque mais comum é a invasão, que em geral tem como objetivo roubar dados sigilosos (geralmente o objetivo é atacar instituições financeiras para obter lucros) ou estragar o funcionamento da página (o que pode ser feito através da exclusão de arquivos).

No caso do ataque realizado pelo grupo Lulz Security Brazil, não foi exatamente uma invasão, mas sim um ataque distribuído por negação de serviço. Esse tipo de ataque não visa roubar dados (em um primeiro momento), porém tem como objetivo retirar determinado site do ar temporariamente sem causar grandes danos. Os objetivos por trás do ataque como o que aconteceu podem ser muitos, desde uma reinvindicação política até atividades criminosas.

O ataque distribuído por negação de serviço (DDoS, do inglês Distributed Denial-of-Service attack) atinge sua meta excedendo os limites do servidor. Para tal façanha, os responsáveis pelo ataque criam programas maliciosos que são instalados em diversas máquinas, as quais realizarão múltiplos acessos simultâneos ao site em questão.



E como os servidores possuem limitações com relação ao número de acessos em um mesmo instante, acaba ocorrendo que o servidor não aguenta atender as requisições e é retirado do ar. Um ataque distribuído por negação de serviço pode simplesmente reiniciar os servidores ou pode causar o travamento total do sistema que opera por trás do site.

Os zumbis também têm culpa

Para aumentar a eficácia do ataque, um DDoS muitas vezes conta com a ajuda de máquinas zumbis, que integram uma rede zumbi. Computadores desse tipo foram infectados por pragas que tornam o acesso à internet extremamente lento, isso porque eles estão sob o comando de outra máquina, também conhecido como computador-mestre.

E justamente por contar com uma legião de máquinas atacando é que os DDoS têm grande eficiência. Por se tratar de milhares computadores realizando o ataque, fica muito mais difícil combatê-lo, porque os responsáveis pela segurança do servidor não conseguem estabelecer regras para impedir todos os acessos que estão causando danos.

Tentando resolver o problema

Para tentar combater um ataque distribuído por negação de serviço, os profissionais que trabalham contra o ataque precisam efetuar configurações nos equipamentos que levam até o site desejado. Em geral, são utilizados filtros que vão determinar quais IPs podem acessar o site e quais são perigosos para o servidor.

Outra solução é recorrer a empresas especializadas, como a Akamai, que utilizam diversos computadores para conter o ataque. Essa técnica é efetiva porque as máquinas estão em diferentes locais do planeta e combatem os zumbis dividindo a tarefa, de modo que cada computador de defesa combata um número reduzido de máquinas.

O ataque pode continuar

O governo brasileiro já divulgou que conteve os ataques realizados em todos os sites, todavia, os responsáveis pelo DDoS podem realizar novos ataques iguais aos que efetuaram ou até piores — invasões dos servidores são bem prováveis. Detectar outros ataques distribuídos por negação de serviço deve ser mais fácil daqui para frente, entretanto, os hackers podem utilizar técnicas ainda mais aperfeiçoadas para futuras atividades contra o governo.

Claro que o assunto DDoS é muito mais complexo do que abordamos aqui, porém, o objetivo era passar uma noção básica do que está acontecendo por trás dos ataques recentes. Você tem algo a acrescentar? Deixe seu comentário!