Ataques DDoS

Como manter minha empresa **segura?**

WCS
CONECTOLOGIA

Ataques DDoS

Como manter minha empresa segura?

As diversas mudanças e adaptações no uso da Internet causadas pela pandemia da COVID-19, como o crescimento do número de funcionários remotos e de acessos durante o *lockdown*, resultaram em um aumento proporcional dos crimes cibernéticos, inclusive de ataques DDoS (Negação de serviço distribuída).

Se você não está familiarizado com o termo, Ataque Distribuído de Negação de Serviço (ou *Distributed Denial of Service* – DDoS, em inglês) tem como objetivo tornar um servidor ou uma infraestrutura indisponíveis, sobrecarregando-os por meio de um comportamento anormal no tráfego de rede. Diversos pedidos são enviados ao mesmo tempo, a partir de vários pontos da Internet, e por conta desta sobrecarga de chamados, o serviço se torna instável, ou no pior cenário, indisponível.

⚠ Durante a pandemia, ataques de DDoS saltam 524%

Os ataques DDoS e o vazamento de dados aumentaram muito, principalmente durante a pandemia e a adesão ao *home office*. Isso porque, os acessos a dados e informações das empresas por meio de diferentes dispositivos, longe da infraestrutura empresarial, como os computadores pessoais, aumentaram a vulnerabilidade de corporações, uma vez que as redes domésticas são menos seguras, tornando, portanto, mais fácil atacar os sistemas das empresas. De acordo com o relatório da *NSFOCUS "2020 Mid-Year DDoS Attack Landscape Report*", O Brasil foi o 4º país que mais sofreu com ataques DDoS, ficando atrás somente de Japão, China e Estados Unidos.

Como funciona um ataque DDoS

Diferente de outros tipos de ataques *hackers* mais conhecidos, o DDoS não tem como objetivo principal roubar dados e informações, mas sim tornar indisponível um servidor através da sobrecarga, fazendo com que os sites fiquem mais lentos ou até mesmo indisponíveis. Entretanto, o DDoS pode ser utilizado em invasão de uma rede ou serviço menos protegido. Assim que o servidor cai, é ativado um DNS* "falso" no site ou *host*, imitando a tela de *login* da empresa, fazendo com que o usuário entre com dados sensíveis, como senhas ou e-mails. Servidores DNS (*Domain Name System*, ou sistema de nomes de domínios) são os responsáveis por localizar e traduzir para números IP os endereços dos sites que digitamos nos navegadores.

A efetividade do DDoS se caracteriza graças ao envio massivo de pacotes ao servidor alvo, aumentando o tráfego de dados a ponto de causar o esgotamento da banda para outros usuários, levando à indisponibilidade do serviço. O atacante consegue esse volume tão grande de envio de pacotes porque utiliza várias máquinas para executar tal ação. Essa estratégia é conhecida como *botnet*, um número de dispositivos conectados à Internet, cada um executando um ou mais *bots*.

Tipos de DDOS

Confira agora algumas técnicas utilizadas:

Ataques volumosos ou Flood

São os tipos mais básicos e comuns de ataques DDoS. Solicitações de acesso são enviadas em larga escala, congestionando a sua largura de banda e deixando-o inacessível na internet.

UDP Flood

O UDP Flood é um tipo de ataque DDoS que inunda portas aleatórias de um alvo com pacotes UDP (*User Datagram Protocol*). O UDP é um protocolo de comunicação que serve para enviar muitos pacotes de informações e receber respostas de uma maneira mais rápida. A partir do momento em que um servidor recebe uma enxurrada de informações, e precisa continuamente checar sua integridade e respondê-las de volta ao solicitante, ele vai ficando mais lento, até sobrecarregar por completo e ficar indisponível para acesso.

NTP Flood

Os invasores enviam pacotes válidos, porém, falsificados, de NTP (*Network Time Protocol*) a um alvo de destino. Como estas solicitações parecem ser verdadeiras, os servidores NTP da vítima continuam tentando responder à grande quantidade de solicitações recebidas. Os recursos dessa rede, então, se esgotam por não resistirem à solicitação, e entram num fluxo de reinicialização repetitiva do sistema, deixando ele, simplesmente, fora do ar.

Zombie Flood

O ataque Zombie Flood é quando conexões vindas de diversas origens extravasam os serviços, provocando paralisia da rede, utilizando conexões com comportamento similar ao de um usuário autêntico.

Alvos típicos de DDoS

E-commerces /lojas virtuais;

Empresas, instituições e associações que dependem de serviços digitais;

Por que alguém colocaria um DDoS no seu site?

São diversas as razões pelas quais um atacante pode querer bombardear seu site por meio de um ataque DDoS. Costumam partir, principalmente, de ataques dos concorrentes e ataques por causa do seu conteúdo, roubo de informações de contatos, vendas, contratos e muito mais.

Ataques DDoS pelos concorrentes

Um concorrente pode contratar alguém para montar um ataque DDoS na rede da sua empresa, sabendo que isso não só terá impacto no seu site, mas também no seu negócio.

DDoS ataca o seu conteúdo

Determinados sites estão sujeitos a ataques DDoS em virtude da natureza de seu conteúdo. O seu conteúdo pode ser comercial, mas ainda assim sensível e podem existir pessoas que não o querem disponível on-line.

Ransomware desliga principal sistema de gasoduto dos EUA

Um ataque cibernético desligou o principal sistema de gasoduto da Costa Leste dos Estados Unidos, no último dia 7 de maio. A ação paralisou o fluxo de combustíveis a ponto de fazer o governo americano declarar emergência em algumas regiões do país.

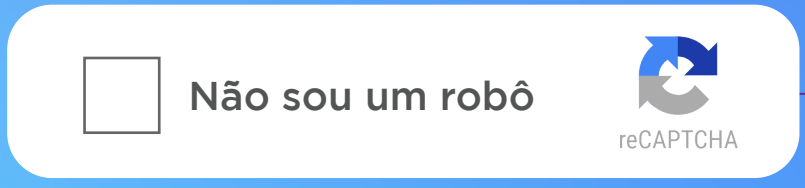
Um grupo de hackers desconectou completamente a rede do gasoduto e roubou mais de 100 GB de informações da empresa Colonial. O duto é responsável por transportar mais de 2,5 milhões de barris de óleo por dia, o que corresponde a 45% do abastecimento de diesel, gasolina e querosene de aviação da costa leste dos EUA.

Como se proteger?

A segurança cibernética deve ser uma preocupação constante de todos, tanto empresas quanto colaboradores. E, se pensarmos na atual situação do mundo, é essencial ampliar ainda mais os cuidados. Para conter e solucionar ataques DDoS, principalmente aqueles que são aplicados em alta escala, você precisará contar com soluções e plataformas de infraestrutura com alta performance.

Como os ataques DDoS visam sobrecarregar o servidor, ter uma infraestrutura robusta e grande largura de banda pode ajudar a evitar que os ataques sejam efetivos. *Firewalls* também são uma excelente forma de proteção, uma vez que eles controlam os acessos e evitam que esse tipo de solicitação em massa possa chegar ao seu servidor. Caso sua empresa utilize formulários, passe a incluir o **reCAPTCHA**, o que ajuda a evitar que *bots* façam um número massivo de inscrições e comprometam o seu servidor.

Se possível, compre também mais velocidade para sua conexão e tenha sempre rotas alternativas, caso a conexão principal seja afetada. Faça uma auditoria periódica das máquinas à procura de portas suspeitas ou programas não-autorizados. Caso você seja um usuário comum, atente-se às principais dicas: não repita senhas, cuidado com links suspeitos e faça o possível para evitar que os seus dispositivos se tornem parte de uma *botnet*.



Anti-DDoS
WCS Conectologia

Mantenha a sua empresa **protegida** contra **ataques cibernéticos!**

Tenha uma rede de segurança para evitar que suas operações sejam afetadas. O Anti-DDoS da WCS Conectologia é uma solução de monitoramento que detecta ataques volumétricos na sua rede, separando o tráfego legítimo do ilícito, protegendo redes de ataques e garantindo a disponibilidade dos serviços. As vantagens são diversas: disponibilidade, alta proteção, latência minimizada e baixo custo operacional.

Entre em contato com WCS Conectologia e conheça nossas soluções de segurança para proteger sua empresa nos meios digitais!

WCS
CONECTOLOGIA