

Desvendando o Caos: A Arte de Sobrecarregar com DDoS

Introdução ao Caos Digital



DDoS (Distributed Denial of Service) é um ataque que busca **sobrecarregar** sistemas, causando interrupções. Nesta apresentação, iremos explorar a **arte** por trás desses ataques, suas **consequências** e como se proteger deles.



O que é DDoS?

O DDoS é um tipo de ataque cibernético que visa tornar um website, servidor ou serviço indisponível ao sobrealarcar os recursos do sistema alvo. Neste ataque, múltiplos dispositivos comprometidos, conhecidos como bots ou zumbis, são utilizados para inundar a rede com um tráfego massivo. O objetivo é deleitar os usuários legítimos e impedir o acesso ao serviço.

Tipos de Ataques DDoS



Existem diversos tipos de ataques **DDoS**, como **UDP Flood**, e **HTTP Flood**. Cada um tem sua **estratégia** e impacto específico. Conhecer essas variações ajuda a **identificar** e **mitigar** os riscos associados.

Motivações por trás dos DDoS



Os ataques **DDoS** podem ser motivados por **razões** políticas, financeiras ou até mesmo por **diversão**. Grupos hacktivistas e cibercriminosos utilizam essas táticas para **promover** suas agendas ou extorquir empresas. Entender essas motivações é crucial.

Impacto nos Negócios

Os efeitos de um ataque **DDoS** podem ser devastadores para empresas, resultando em **perdas** financeiras, danos à **reputação** e perda de **clientes**. A continuidade dos negócios é ameaçada, e a recuperação pode ser um processo longo e caro.

Exemplo: Imagine se, a varejista Magazine Luiza, por alguma falha de sistema mantivesse sua plataforma fora do ar por algumas horas ou minutos, onde a maior parte do faturamento da empresa é na plataforma online.



Casos Famosos de DDoS



Anonymous reivindica responsabilidade por ataque cibernético no Departamento de Polícia de Minneapolis. O ataque ocorreu após a brutal morte de George Floyd nas mãos da polícia de Minneapolis. Após o ocorrido, os invasores, derrubaram diversos sites do governo Americano, incluindo o site de Departamento de Polícia de Minneapolis, onde foi utilizado o DDoS, mantendo a plataforma fora de serviço. "O Security Operations Center do MNIT está se defendendo contra ataques cibernéticos de negação de serviço distribuída (DDOS) que visam sobrecarregar os sistemas de informação e redes estaduais para deixá-los offline", disse Tarek Tomes, CIO do estado e comissário de Serviços de TI de Minnesota (MNIT), a um jornal local.

Para se proteger contra ataques DDoS, as empresas podem implementar **firewalls**, **sistemas de detecção** e serviços de mitigação.





A Importância da Prevenção

Prevenir ataques **DDoS** é mais eficaz do que responder a eles. Investir em **infraestrutura** sólida e em **treinamento** de equipe pode reduzir significativamente os riscos. A **educação** sobre segurança cibernética é uma prioridade.

Existem várias **ferramentas** disponíveis para ajudar a mitigar ataques DDoS, como **Cloudflare**, **Akamai** e **Imperva**. Essas soluções oferecem **proteção** em tempo real.



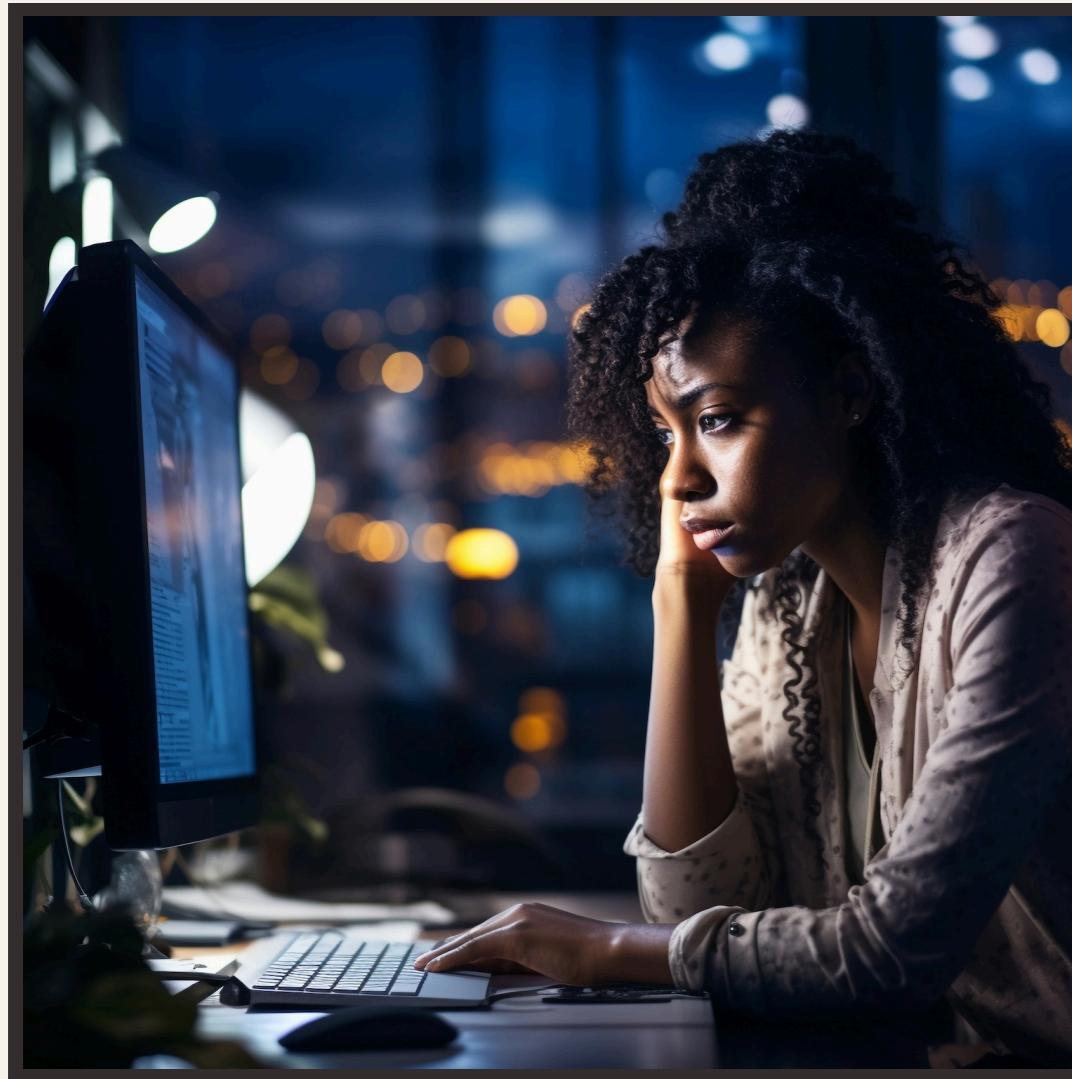
Conclusão: Enfrentando o Caos

É importante o conhecimento e entendimento do assunto para ter boas técnicas de prevenção a esse tipo de ataque, pois mesmo utilizando as medidas de segurança ainda há o risco desse ataque.



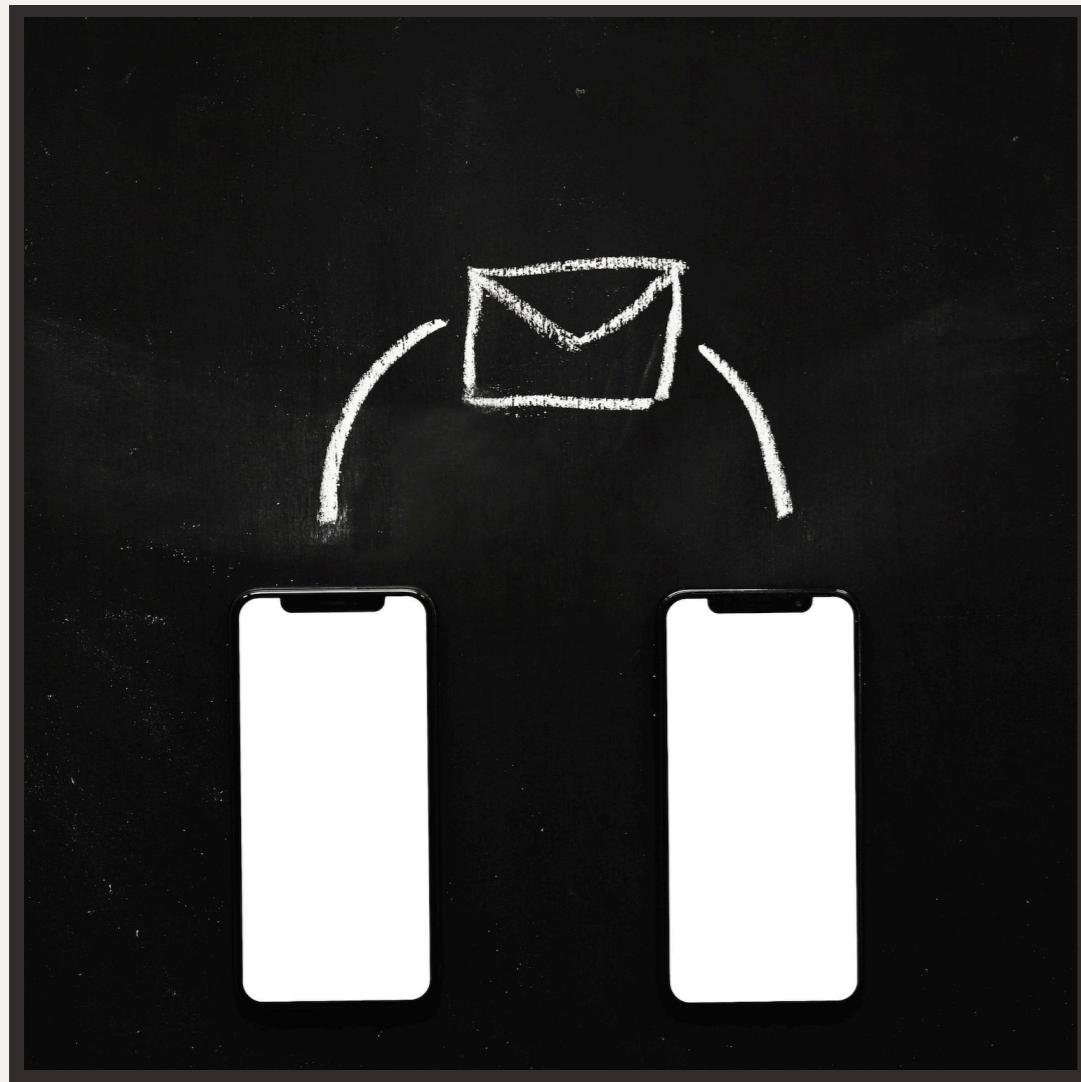
Desvendando as Armadilhas: Como Não Cair nas Redes do Phishing

Introdução ao Phishing



O **phishing** é uma técnica de **fraude digital** que visa enganar usuários para obter informações pessoais. Neste slide, vamos explorar como essas armadilhas funcionam e como podemos nos proteger.

Tipos Comuns de Phishing



Existem vários tipos de **phishing**, como **phishing por e-mail**, **smishing** (SMS) e **vishing** (voz). Cada um tem suas características, mas todos têm o mesmo objetivo: **enganar** você. Conhecer esses tipos é o primeiro passo para se proteger.

O ataque ao Banco do Brasil em 2020



Em 2020, o Banco Central do Brasil foi alvo de um sofisticado ataque de phishing que resultou na transferência de cerca de R\$ 3 milhões para contas bancárias controladas pelos criminosos.

Os golpistas enviaram e-mails falsos para funcionários do banco, solicitando a atualização de informações de login em um sistema interno.

Metódo: Ao clicarem no link fornecido no e-mail, os funcionários foram direcionados para um site falso que se assemelhava à página de login do sistema interno do banco. Ao inserir suas informações de login, os golpistas conseguiram obter acesso às contas dos funcionários e realizar transferências fraudulentas.



CRISIS



Consequências

A violação de dados comprometia a segurança e a integridade das operações do Banco Central, o que poderia afetar a confiança pública na instituição e na estabilidade financeira.



Lição

Implementou medidas para reforçar a segurança, incluindo a atualização de protocolos de segurança, a aplicação de patches e a realização de treinamentos de conscientização sobre segurança para os funcionários.

Agradeçemos pela
atenção :)

FONTES:

<https://www.govtech.com/security/anonymous-claims-responsibility-for-minneapolis-pd-cyberattack.html#:~:text=The%20Minneapolis%20city%20and%20police,it%20stole%20from%20the%20city.>

<https://www.cloudflare.com/pt-br/learning/ddos/what-is-a-ddos-attack/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6389>

<https://www.remessaonline.com.br/blog/banco-do-brasil-no-exterior/>