UNIVERSIDADE DE BRASÍLIA

Faculdade do Gama

Sistemas de Banco de Dados 2

Trabalho Final (TF)

Problemas de Segurança e Invasões em Banco de Dados

Ransomware e DDOS

Cainã Valença de Freitas 18/0014412

Brasília, DF

2023

a) Definição da Tecnologia Pesquisada

Ransomware e ataques DDoS (Distributed Denial of Service) são duas formas distintas de ameaças cibernéticas que podem afetar bancos de dados.

Para Alves e Pedrosa (2016): “O ransomware é um tipo de malware que usa técnicas de criptografia para bloquear os arquivos e sistemas de uma vítima. O atacante exige um resgate da vítima, prometendo restaurar o acesso aos dados após o pagamento”

De acordo com Pinheiro (2012), um ataque DDoS é definido da seguinte forma: "Um ataque de negação de serviço distribuído (DDoS) ocorre quando um atacante sobrecarrega uma rede ou um alvo específico com uma quantidade massiva de tráfego de diversas fontes para interromper sua operação normal. O objetivo é tornar o serviço indisponível para seus usuários pretendidos"

Ransomware e ataques DDoS são duas formas de ameaças cibernéticas que podem afetar bancos de dados. O ransomware é um tipo de malware que criptografa ou bloqueia os dados da vítima, exigindo um resgate para restaurar o acesso. Os ataques DDoS têm como objetivo sobrecarregar a rede ou o site alvo com tráfego intenso, tornando o serviço indisponível para os usuários legítimos. Ambas ameaças têm impactos significativos na acessibilidade dos dados e na disponibilidade dos serviços relacionados aos bancos de dados.

b) Objetivo(s) principal(is) da Tecnologia Pesquisada

Ransomware e ataques DDoS apesar de serem duas ameaças cibernéticas que tem origem em um atacante malicioso, possuem objetivos diferentes.

Os principais objetivos de um ransomware em relação a um banco de dados são o sequestro e a extorsão dos dados armazenados no banco de dados, com o intuito de obter um pagamento financeiro (ransom) em troca da liberação dos dados. Especificamente, o ransomware visa criptografar os arquivos do banco de dados, tornando-os inacessíveis para os usuários legítimos, e exige o pagamento de um resgate em criptomoedas para fornecer a chave de descriptografia. Uma vez que um ransomware infecta um sistema que contém um banco de dados, ele pode comprometer não apenas os dados em si, mas também a disponibilidade e a integridade dos dados. Os atacantes podem impedir que os usuários acessem seus dados e exigir um resgate para restaurar o acesso. Além disso, eles podem ameaçar vazar os dados confidenciais caso o pagamento não seja realizado.

Os principais objetivos de um ataque de negação de serviço distribuído (DDoS, do inglês Distributed Denial of Service) em relação a um banco de dados são interromper ou prejudicar a disponibilidade do banco de dados, tornando-o inacessível aos usuários legítimos. Em um ataque DDoS, um grande volume de tráfego malicioso é direcionado ao banco de dados, sobrecarregando seus recursos e prejudicando seu funcionamento normal. Ao inundar o banco de dados com uma quantidade excessiva de solicitações, um ataque DDoS pode levar ao congestionamento do sistema, esgotamento de recursos como memória, processamento ou largura de banda, tornando-o incapaz de atender às solicitações legítimas dos usuários. Isso resulta em indisponibilidade temporária ou completa do banco de dados, causando interrupção nos serviços e prejuízos financeiros para a organização.

c) Vantagens da Tecnologia Pesquisada;

Ransomware e ataques DDoS possuem diferentes vantagens, tanto para atacantes maliciosos, quanto para organizações privadas e para atacantes do governo (policiais, peritos, militares etc)

Vantagens do Ransomware:

1. Potencial de lucro: O ransomware oferece aos criminosos a oportunidade de obter lucros substanciais por meio de pagamentos de resgate (ransom). Os valores exigidos podem variar de algumas centenas a milhares ou até mesmo milhões de dólares, dependendo da importância dos dados sequestrados.
2. Anonimato: Os atacantes podem usar métodos de pagamento anônimos, como criptomoedas, para dificultar o rastreamento de suas identidades.
3. Facilidade de distribuição: O ransomware pode ser disseminado de várias maneiras, incluindo e-mails de phishing, downloads maliciosos e vulnerabilidades de software, permitindo que os criminosos alcancem um grande número de vítimas.

Vantagens do DDoS:

1. Dificulta o acesso aos serviços: Um ataque DDoS bem-sucedido pode tornar um serviço indisponível para os usuários legítimos, prejudicando a concorrência ou interrompendo as operações de uma organização.
2. Desvio de atenção: Enquanto uma organização está lidando com um ataque DDoS, os atacantes podem aproveitar a distração para realizar outras atividades maliciosas, como invasões, roubo de dados ou até mesmo um ransomware.
3. Dificuldade de atribuição: Devido à natureza distribuída dos ataques DDoS, é mais difícil identificar e atribuir responsabilidade aos atacantes.

d) Desvantagens da Tecnologia Pesquisada;

Desvantagens do Ransomware:

1. Impacto negativo na reputação: As organizações afetadas pelo ransomware podem sofrer danos significativos à sua reputação, perdendo a confiança dos clientes e parceiros de negócios.
2. Perda de dados: Em alguns casos, mesmo que o pagamento do resgate seja feito, não há garantia de que os criminosos fornecerão a chave de descriptografia ou que os dados não tenham sido corrompidos durante o processo de criptografia.
3. Custos de recuperação: Além do pagamento do resgate, vítimas de ransomware podem enfrentar custos adicionais relacionados à restauração de sistemas, investigação forense digital e implementação de medidas de segurança adicionais.

Desvantagens do DDoS:

1. Perda financeira: Empresas que dependem da disponibilidade online de seus serviços podem sofrer perdas financeiras significativas durante um ataque DDoS devido à interrupção dos negócios.
2. Danos à reputação: A indisponibilidade prolongada de serviços pode afetar negativamente a reputação de uma organização, levando à perda de clientes e de confiança no mercado.
3. Colateralidade: Às vezes, um ataque DDoS pode afetar indiretamente outros sistemas e serviços compartilhados, prejudicando usuários e organizações que não eram o alvo original.

Por serem técnicas diferentes, Ransomware e ataques DDoS possuem diferentes desvantagens, tendo em comum a óbvia desvantagem do risco de ser preso ao usar essas técnicas de forma ilegal.

e) Exemplo(s) de uso interessante(s) em empresas, organizações, projetos ou instituições dessa tecnologia de Banco de Dados pesquisada;

Nos últimos anos, o cenário de segurança cibernética testemunhou um aumento nos ataques devastadores, como os ataques de negação de serviço distribuídos (DDoS) e os incidentes de ransomware.

Um dos ataques DDoS mais infames ocorreu em 2016, quando a botnet Mirai desencadeou o caos na Dyn, um renomado provedor de serviços de DNS. Esse ataque interrompeu os serviços de internet por várias horas, tornando temporariamente inacessíveis sites populares como Twitter, Netflix e Spotify para usuários em todo o mundo.

Outro exemplo de ataque DDoS que merece destaque ocorreu em 2018, quando o GitHub, uma plataforma popular de hospedagem de código, foi alvo de um ataque massivo. O ataque atingiu um pico de 1,35 terabits por segundo (Tbps), causando interrupções temporárias no acesso aos serviços do GitHub.

Desviando nosso foco para o ransomware, o ataque WannaCry em 2017 se espalhou rapidamente, infectando centenas de milhares de computadores em 150 países. Aproveitando vulnerabilidades nos sistemas Microsoft Windows, o WannaCry criptografou arquivos em máquinas comprometidas e exigiu pagamentos de resgate em Bitcoin, deixando as vítimas em um estado de paralisia digital.

Pouco depois do WannaCry, outro ataque de ransomware chamado NotPetya causou estragos em escala global. Originário de um software de contabilidade ucraniano comprometido chamado M.E.Doc, o NotPetya infectou rapidamente milhares de sistemas em todo o mundo, perturbando setores vitais, como transporte, bancário e saúde. O ataque aproveitou a vulnerabilidade EternalBlue, originalmente desenvolvida pela Agência de Segurança Nacional (NSA) e posteriormente vazada para o público.

Esses exemplos servem como um lembrete assustador das ameaças cibernéticas em constante evolução enfrentadas por indivíduos, organizações e

até mesmo nações inteiras. À medida que o mundo digital continua a se expandir, é crucial permanecer vigilante e implementar medidas de segurança robustas para proteger-se contra o perigo sempre presente de ataques DDoS e infiltrações de ransomware.

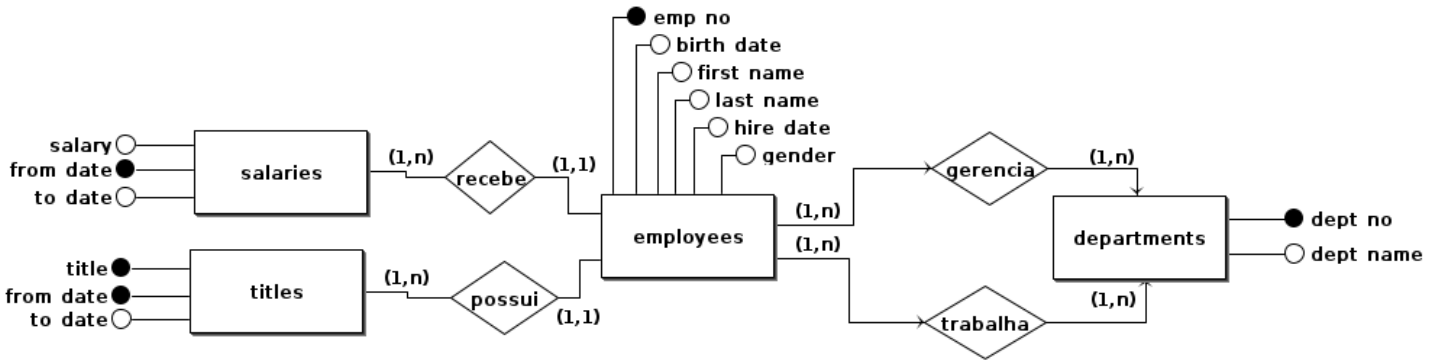
f) Bibliografias Pesquisadas

- Alves, N. M. R., & Pedrosa, R. M. (2016). Segurança de Computadores: Tecnologia e Práticas de Redes. Novatec Editora.
- Pinheiro, J. M. S. (2012). Segurança da Informação: Princípios e Práticas. Brasport.
- Dyn DDoS (2016). https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
- GitHub DDoS (2018). https://github.blog/2018-03-01-ddos-incident-report/
- WannaCry (2017). https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry
- NotPetya (2017). https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

g) Base de Dados (documentação)

A base de dados escolhida para essa etapa foi a base de dados de empregados fornecida como amostra pela no site do mysql (https://dev.mysql.com/doc/employee/en/)

DER:



DLD: