# Atividade Proposta: Análise de Ataques Cibernéticos

## Introdução

Este documento apresenta uma análise detalhada de dois ataques cibernéticos de grande repercussão ocorridos nos últimos cinco anos, conforme solicitado na atividade. Os ataques escolhidos foram o ataque de ransomware contra a **Colonial Pipeline** e o ataque à cadeia de suprimentos da **SolarWinds (SUNBURST)**, selecionados por representarem tipos distintos de ameaças e por seus impactos significativos em infraestruturas críticas e na segurança global.

## Ataque 1: Colonial Pipeline

**1. Data do ataque:**

O ataque foi descoberto e iniciado em 7 de maio de 2021.

**2. Tipo de ataque:**

Ransomware, um tipo de ataque em que os dados da vítima são criptografados e um resgate é exigido para restaurar o acesso.

**3. Descrição do ataque ou de como aconteceu:**

O grupo cibercriminoso conhecido como DarkSide obteve acesso à rede de tecnologia da informação (TI) da Colonial Pipeline, a maior operadora de oleodutos dos Estados Unidos. A invasão ocorreu por meio de uma única credencial de VPN (Rede Privada Virtual) que foi comprometida. Essa conta, pertencente a um ex-funcionário, não estava protegida por autenticação multifator (MFA). Uma vez dentro da rede, os invasores implantaram o ransomware, criptografaram aproximadamente 100 GB de dados e os exfiltraram (roubaram). Diante da ameaça, a Colonial Pipeline desligou preventivamente toda a sua operação de oleodutos para evitar que o ataque se espalhasse para os sistemas de controle operacional (OT), causando uma paralisação massiva no fornecimento de combustível na costa leste dos EUA.

**4. Vulnerabilidade explorada (verificar se está no CVE e qual o seu código):**

O ataque não explorou uma vulnerabilidade de software específica com um código CVE. A principal vulnerabilidade foi uma falha grave de segurança operacional e de gestão de identidade. O ponto de entrada foi uma senha comprometida para uma conta VPN, que foi encontrada em um vazamento de dados na dark web. A ausência de autenticação multifator (MFA) foi o fator decisivo que permitiu o sucesso do acesso inicial.

**5. Impactos e/ou prejuízo (pode ser estimado):**

* **Impacto na Infraestrutura Crítica:** A paralisação do oleoduto por quase uma semana gerou uma crise de abastecimento de combustível, levando a compras de pânico, aumento de preços e declarações de estado de emergência.
* **Prejuízo Financeiro:** A Colonial Pipeline pagou um resgate de 75 bitcoins, que na época valiam cerca de **US$ 4,4 milhões**. Embora parte desse valor tenha sido recuperado pelo FBI, os custos totais com a resposta ao incidente, perda de receita e investimentos em segurança foram muito superiores.
* **Impacto na Segurança Nacional:** O incidente expôs a vulnerabilidade da infraestrutura crítica dos EUA a ataques cibernéticos, levando a novas diretrizes de segurança do governo.

**6. Tipo de Proteção que poderia ter sido aplicada para evitá-lo:**

* **Implementação de Autenticação Multifator (MFA):** Medida mais crucial. Teria bloqueado o acesso inicial, mesmo com a senha comprometida.
* **Gestão de Identidade e Acesso (IAM):** Desativação imediata de contas de ex-funcionários.
* **Segmentação de Rede:** Uma separação mais robusta entre as redes de TI (corporativa) e OT (operacional) poderia ter limitado o risco e evitado a necessidade de um desligamento completo da operação.
* **Monitoramento e Detecção de Ameaças:** Sistemas para detectar atividades anômalas, como logins de contas inativas ou a movimentação de grandes volumes de dados.

## Ataque 2: SolarWinds (SUNBURST)

**1. Data do ataque:**

A violação foi descoberta em dezembro de 2020, mas a infiltração inicial e a distribuição do código malicioso começaram meses antes, por volta de março de 2020.

**2. Tipo de ataque:**

Ataque à Cadeia de Suprimentos (Supply Chain Attack), onde um fornecedor de software é comprometido para distribuir malware aos seus clientes.

**3. Descrição do ataque ou de como aconteceu:**

Os invasores, atribuídos ao grupo de elite APT29 (Cozy Bear), patrocinado por um estado-nação, comprometeram o ambiente de desenvolvimento da SolarWinds. Eles inseriram um código malicioso (um backdoor chamado "SUNBURST") em uma atualização legítima do software de monitoramento Orion Platform. Quando a SolarWinds enviou essa atualização para milhares de seus clientes — incluindo agências do governo dos EUA e grandes empresas —, eles inadvertidamente instalaram o malware. O backdoor se comunicava com servidores de Comando e Controle (C2) dos invasores, permitindo-lhes roubar dados, espionar as redes das vítimas e implantar outros malwares para aprofundar o comprometimento.

**4. Vulnerabilidade explorada (verificar se está no CVE e qual o seu código):**

O ataque em si foi complexo e não se baseou em uma única vulnerabilidade CVE para o acesso inicial. No entanto, o backdoor implantado foi rastreado como CVE-2020-10148. Além disso, uma vez dentro das redes das vítimas, os invasores exploraram outras falhas. Uma delas, relacionada à plataforma Orion, é a CVE-2020-14005, que permitia a um invasor contornar a autenticação. O principal vetor, contudo, foi o comprometimento do processo de build do software.

**5. Impactos e/ou prejuízo (pode ser estimado):**

* **Impacto Estratégico e de Espionagem:** Considerado um dos ataques de espionagem cibernética mais significativos da história, comprometendo agências governamentais de alto escalão e grandes empresas de tecnologia.
* **Vazamento de Dados Sensíveis:** Roubo de informações confidenciais, propriedade intelectual e comunicações internas de centenas de organizações.
* **Prejuízo Financeiro:** O custo global para remediar o ataque foi estimado em mais de **US$ 100 bilhões**, incluindo custos de investigação, limpeza de redes, melhorias de segurança e perda de confiança no mercado. As ações da SolarWinds despencaram após a revelação.

**6. Tipo de Proteção que poderia ter sido aplicada para evitá-lo:**

* **Segurança no Ciclo de Vida de Desenvolvimento de Software (Secure SDLC):** Implementação de processos rigorosos de verificação de integridade do código, assinatura de código e monitoramento contínuo do ambiente de desenvolvimento.
* **Princípio do Mínimo Privilégio:** Limitar permissões de sistemas e usuários para conter o dano em caso de comprometimento.
* **Monitoramento de Rede Avançado:** Uso de ferramentas de EDR (Endpoint Detection and Response) e NDR (Network Detection and Response) para identificar comunicações suspeitas com servidores C2 e outras atividades anômalas.
* **Zero Trust Architecture:** Adotar um modelo de "confiança zero", onde nenhum usuário ou dispositivo é confiável por padrão, exigindo verificação contínua.