Renata Cristina Niedsviecki Pereira

824144772

Rebeca Barcelos Rocha Carneiro

RA: 824148696

**1. Ataque ao Colonial Pipeline (Maio de 2021)\*\***

**Tipo de Ataque:** Ransomware (DarkSide)

**Descrição:**  Em maio de 2021, o sistema da Colonial Pipeline, uma das maiores redes de oleodutos dos EUA, foi paralisado por um ataque de ransomware. Os atacantes usaram malware para criptografar dados críticos e exigir resgate em criptomoeda para a restauração do sistema.

**Vulnerabilidade Explorada:** A vulnerabilidade específica não foi identificada publicamente no CVE, mas o ataque ocorreu por meio de uma senha comprometida associada a uma conta de VPN desativada que não utilizava autenticação multifator (MFA).

**Impactos** :O ataque causou a paralisação total do oleoduto por cinco dias, resultando em falta de combustível em várias regiões dos EUA. A empresa pagou um resgate de cerca de $4,4 milhões, dos quais $2,3 milhões foram posteriormente recuperados pelo governo.

**Proteção Aplicável:** O uso de autenticação multifator (MFA) e o gerenciamento mais rigoroso de contas inativas poderiam ter prevenido o ataque. Medidas de segurança em redes, como segmentação e detecção avançada de malware, também teriam sido eficazes.

---

**2. Ataque ao SolarWinds (Dezembro de 2020)**

**Tipo de Ataque:** Supply Chain (Ataque à cadeia de suprimentos)

**Descrição**:O ataque ao SolarWinds foi uma das maiores e mais sofisticadas operações de espionagem cibernética já registradas. Hackers infiltraram o software de gerenciamento de rede Orion da SolarWinds e distribuíram uma atualização infectada, comprometendo as redes de empresas e agências governamentais dos EUA.

**Vulnerabilidade Explorada:** A vulnerabilidade primária explorada foi a inserção de código malicioso no ciclo de desenvolvimento do software Orion. Não há um código CVE específico associado a este ataque, pois se tratou de uma falha na cadeia de suprimentos.

**Impactos:** Aproximadamente 18.000 clientes da SolarWinds baixaram a atualização comprometida. O ataque afetou várias agências governamentais e empresas privadas. Estima-se que o prejuízo tenha sido de bilhões de dólares, considerando os custos de mitigação e investigação.

**Proteção Aplicável:** Uma maior vigilância no processo de desenvolvimento e distribuição de software, com auditorias de código-fonte e verificação de integridade das atualizações, poderia ter evitado o ataque. O uso de assinaturas digitais para verificar a autenticidade do software também seria eficaz.

---

Esses dois exemplos mostram como diferentes vulnerabilidades, desde falhas humanas até explorações na cadeia de suprimentos, podem resultar em grandes prejuízos financeiros e de infraestrutura. Implementar controles de segurança robustos e manter boas práticas pode ajudar a prevenir esses ataques.