Integrantes Do Grupo

Otavio Paiva/ RA: 824147017
Gabriel Prieto/ RA: 824142064
Eduardo Baptistella/ RA: 824147595

**1. Ataque de Ransomware - "WannaCry" (2017)**

Data do ataque:

Data: 12 de maio de 2017

Tipo de ataque:

Tipo de ataque: Ransomware

**Descrição da agressão:**

O WannaCry foi um ataque de ransomware que se propagou rapidamente entre computadores globais, explorando uma falha no sistema operacional Windows. O ransomware aproveitou uma brecha no Windows SMB (Bloqueio de Mensagens do Servidor), que possibilita a execução de código de forma remota em sistemas suscetíveis. Depois de infectados, os sistemas comprometidos tiveram seus dados codificados e uma solicitação de pagamento em Bitcoin para a devolução das informações.

Exploração de vulnerabilidade:

Vulnerabilidade: CVE-2017-0144 - Um erro no serviço SMBv1 do Windows, que possibilita a execução de código de forma remota sem a intervenção do usuário. A NSA desenvolveu o exploit usado no ataque, conhecido como EternalBlue, que foi exposto pelo coletivo Shadow Brokers.

Criptografia: CVE-2017-0144

**Efeitos e/ou danos:**

O incidente prejudicou mais de 200.000 dispositivos em 150 nações.

Hospitais britânicos (NHS), corporações internacionais e estruturas governamentais foram particularmente impactadas.

A perda de dados, interrupções nos serviços e despesas de recuperação resultaram em um impacto financeiro estimado em bilhões de dólares. O NHS do Reino Unido teve que cancelar operações e comprometer serviços essenciais, resultando em uma perda estimada de £92 milhões (aproximadamente US$120 milhões).

Proteção que poderia ter sido implementada para prevenir o incidente:
Atualizações de segurança e correções: A Microsoft disponibilizou um patch de segurança (MS17-010) para resolver a vulnerabilidade no SMBv1, contudo, muitas entidades não implementaram a atualização no devido tempo.
Remoção do SMBv1: A remoção do SMBv1 e a adoção de versões mais seguras do SMB, como SMBv2 ou SMBv3, poderiam ter prevenido o ataque.
Antivírus e sistemas de detecção de invasões: Instrumentos de proteção que rastreiam atividades suspeitas na internet poderiam ter identificado comportamentos incomuns, como tentativas de invasão do EternalBlue.

**2. Ataque de Phishing - "Campanha de Phishing SolarWinds" (2020)**

Data do ataque:

> Data: O ataque foi descoberto em dezembro de 2020, mas acredita-se que tenha ocorrido por vários meses antes disso.

Tipo de ataque:

> Tipo de ataque: Phishing e ataque de cadeia de suprimentos (supply chain attack)

**Descrição do ataque:**

O incidente SolarWinds representou uma grave violação de segurança cibernética, com os atacantes, que provavelmente estavam ligados ao governo russo, comprometendo a plataforma de monitoramento de TI da SolarWinds, utilizada por milhares de entidades globais.

O ataque ocorreu através da inserção de um código malicioso em uma atualização legítima do software Orion da SolarWinds. Isso possibilitou que os invasores tivessem acesso a redes governamentais e empresariais globais. A ação foi simplificada através de métodos de phishing para adquirir credenciais e acessos iniciais.

Apesar do ataque ter como objetivo o dano à cadeia de abastecimento, o phishing foi um dos métodos empregados para disseminar a exploração da vulnerabilidade.

**Vulnerabilidade explorada:**

A falha identificada não foi diretamente no código do software SolarWinds, mas sim na manipulação da cadeia de fornecimento, possibilitando a disseminação do código malicioso como uma atualização legítima.

Contudo, em ataques de phishing, os criminosos também empregaram estratégias de engenharia social para adquirir as credenciais de administradores de sistemas e ampliar a permanência no ambiente comprometido.

**Impactos e/ou prejuízo:**

O ataque impactou mais de 18.000 entidades, englobando órgãos governamentais dos Estados Unidos, como o Departamento de Segurança Interna, além de grandes corporações como Microsoft, Cisco e Intel.

A estimativa exata do impacto financeiro do ataque é complexa, mas a recuperação e a redução dos prejuízos resultaram em centenas de milhões de dólares. Ademais, o ataque prejudicou a confiança nas cadeias de fornecimento de software e revelou dados confidenciais de governos e empresas.

Ademais, a exposição ao ataque foi prolongada, com diversos sistemas comprometidos por meses antes de serem identificados, elevando consideravelmente o custo do ataque.

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

Autenticação multifatorial (MFA): A aplicação do MFA poderia ter dificultado o acesso indevido, mesmo que as credenciais estivessem comprometidas.

Acompanhamento de atividades e avaliação de comportamentos: O emprego de instrumentos sofisticados de monitoramento de rede e identificação de comportamentos atípicos poderia ter detectado rapidamente atividades suspeitas, como a utilização de senhas vulneráveis para acessar sistemas vitais.

Exame e certificação de software: Uma análise mais rigorosa das atualizações de software e a utilização de assinaturas digitais sólidas poderiam ter prevenido a adição do código malicioso nas atualizações da SolarWinds.

Formação em segurança: Programas constantes de capacitação em phishing e engenharia social para colaboradores, especialmente em organizações de alta hierarquia, poderiam ter contribuído para diminuir a efetividade de ataques iniciais de phishing.