

Atividade sobre ataques cibernéticos

Pedro Paulo A. dos Santos - 823217810

1) Ataque à Cadeia de Suprimentos da SolarWinds

Descoberto em dezembro de 2020, o ataque à SolarWinds representou um dos mais sofisticados ataques à cadeia de suprimentos da história. Hackers ligados a um grupo estatal inseriram um código malicioso, conhecido como backdoor "SUNBURST", diretamente nas atualizações do software de gerenciamento de TI da SolarWinds, a Plataforma Orion. Milhares de clientes, incluindo agências do governo dos EUA e grandes corporações, instalaram a atualização infectada, permitindo que os invasores se infiltrassem secretamente em suas redes por meses para realizar espionagem. O ataque explorou a confiança no processo de atualização de software e uma vulnerabilidade específica, a CVE-2020-10148, para obter acesso e se mover lateralmente dentro das redes das vítimas. O impacto foi monumental, com custos de remediação na casa dos bilhões de dólares e uma profunda quebra de confiança na segurança da cadeia de suprimentos de software. A mitigação para tais ataques exige uma abordagem de "confiança zero" (Zero Trust), monitoramento contínuo da rede e um controle de segurança rigoroso nos ambientes de desenvolvimento de software.

Data: Descoberto em dezembro de 2020 (iniciado meses antes).

Tipo de Ataque: Ataque à Cadeia de Suprimentos (Supply Chain Attack).

Descrição: Hackers inseriram um backdoor (SUNBURST) em uma atualização legítima do software Orion da SolarWinds. A atualização maliciosa foi distribuída a milhares de clientes, comprometendo suas redes.

Vulnerabilidade Explorada: Confiança na cadeia de suprimentos de software e a vulnerabilidade **CVE-2020-10148**, que permitia o bypass de autenticação no software Orion.

Impacto e Prejuízo: Comprometimento de até 18.000 organizações, incluindo agências do governo dos EUA e grandes empresas, para fins de espionagem. Prejuízos estimados na casa dos bilhões de dólares.

Proteção Aplicável: Arquitetura de segurança de "confiança zero" (Zero Trust), monitoramento rigoroso da rede e maior segurança no ciclo de vida de desenvolvimento de software.

2) Ataque à Colonial Pipeline

Em maio de 2021, a Colonial Pipeline, operadora do maior oleoduto de combustível dos Estados Unidos, sofreu um devastador ataque de ransomware que paralisou suas operações. O ataque, executado pelo grupo DarkSide, teve origem na exploração de uma única senha comprometida de uma conta de VPN inativa. A principal falha de segurança foi a ausência de autenticação multifator (MFA) nessa conta, o que permitiu aos invasores um acesso fácil à rede de TI da empresa. Uma vez dentro, eles criptografaram dados vitais, forçando a empresa a interromper o fluxo de combustível para toda a Costa Leste dos EUA. O impacto foi severo, causando pânico, escassez de combustível e um prejuízo financeiro significativo, que incluiu o pagamento de um resgate de US\$4,4 milhões. Este incidente poderia ter sido evitado com a aplicação de medidas de segurança básicas, como a implementação obrigatória de MFA em todos os acessos remotos e um gerenciamento mais rigoroso das contas de usuário.

Data: 7 de maio de 2021

Tipo de Ataque: Ransomware

Descrição: Cibercriminosos (grupo DarkSide) usaram uma senha de VPN comprometida para acessar a rede, criptografar arquivos e forçar a paralisação do maior oleoduto de combustível dos EUA.

Vulnerabilidade Explorada: Falha de segurança operacional. Acesso obtido através de uma conta de VPN que não possuía **autenticação multifator (MFA)** ativada.

Impacto e Prejuízo: Paralisação do fornecimento de 45% do combustível da Costa Leste dos EUA, causando escassez e pânico. Pagamento de resgate de **US\$ 4,4 milhões**.

Proteção Aplicável: Implementação de **autenticação multifator (MFA)** em todos os acessos remotos e desativação de contas inativas.