Nome: Beatriz Silva de Jesus

RA: 824219590

Ataque 1: Hot Topic

1. Data do ataque (pode ser aproximada):

O ataque ocorreu entre 7 de fevereiro e 21 de junho de 2023.

2. Tipo de ataque:

O ataque foi um Credential Stuffing (Preenchimento de Credenciais). Neste tipo de ataque, hackers usaram credenciais roubadas de outros vazamentos e tentaram acessar as contas dos clientes na plataforma de recompensas da Hot Topic.

3. Descrição do ataque ou de como aconteceu:

O tipo de ciberataque descrito no texto é o **"Credential Stuffing"** (preenchimento de credenciais). Esse ataque ocorre quando hackers usam credenciais de login (nome de usuário e senha) obtidas de vazamentos anteriores de outros serviços ou sites. Eles testam essas credenciais em diversas plataformas, na esperança de que os usuários reutilizem as mesmas combinações de nome de usuário e senha em diferentes serviços.

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

O ataque descrito é um Credential Stuffing, que não explora diretamente uma vulnerabilidade técnica no software ou sistema (portanto, não há um código CVE específico associado). A vulnerabilidade está no comportamento dos usuários que reutilizam as mesmas credenciais (nomes de usuário e senhas) em várias plataformas, tornando suas contas suscetíveis a ataques após o vazamento de credenciais em outros serviços.

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

O impacto potencial envolve a exposição de informações sensíveis dos clientes da Hot Topic, como os dados das contas de recompensas. O ataque pode resultar em acesso não autorizado a contas, possível roubo de pontos de recompensas ou dados pessoais, danos à reputação da empresa, visto que clientes podem perder confiança em sua segurança, custo financeiro associado à notificação de clientes, suporte técnico, monitoramento e eventuais medidas legais.Os prejuízos podem incluir tanto perdas financeiras quanto danos à imagem da marca, o que pode ser substancial dependendo da quantidade de contas afetadas.

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

Bloqueio de tentativas de login que Implementa uma limitação no número de tentativas de login falhas antes de bloquear a conta temporariamente pode frustrar ataques de força bruta ou stuffing, monitoramento de logins suspeitos para detectar padrões anômalos de login, como várias

Ataque 2: SolarWinds

1. Data do ataque (pode ser aproximada):

O ataque foi descoberto em Dezembro de 2020, mas a invasão começou a ocorrer em Março de 2020, quando os hackers comprometeram as atualizações do software SolarWinds Orion.

2. Tipo de ataque:

O ataque foi um Ataque à Cadeia de Suprimentos (Supply Chain Attack), no qual hackers comprometeram o processo de desenvolvimento de software de um fornecedor (SolarWinds) para distribuir malware para os clientes desse fornecedor.

3. Descrição do ataque ou de como aconteceu:

Os invasores, supostamente associados a um grupo de hackers patrocinado por um Estado (APT), comprometeram o software de monitoramento SolarWinds Orion ao injetar um código malicioso em suas atualizações. Quando clientes legítimos da SolarWinds, incluindo agências governamentais e grandes corporações, aplicaram essas atualizações, o malware foi instalado em suas redes, permitindo que os invasores acessassem sistemas internos sem serem detectados. Esse ataque se espalhou para milhares de empresas e agências governamentais, incluindo órgãos dos Estados Unidos.

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

O ataque explora uma vulnerabilidade relacionada ao comprometimento do processo de desenvolvimento de software, que não tem um CVE diretamente associado, já que o malware foi inserido durante a compilação e distribuição de software legítimo. No entanto, um dos códigos CVE relevantes associados a esse ataque é o CVE-2020-10148, que descreve uma vulnerabilidade que permitia a execução remota de código (RCE) em algumas versões do Orion, facilitando a persistência do ataque.

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

O ataque comprometeu várias agências governamentais dos EUA, incluindo o Departamento do Tesouro e o Departamento de Justiça, bem como grandes corporações. Os impactos foram extensos como roubo de dados sensíveis e acesso a redes críticas de segurança nacional, prejuízos financeiros diretos e indiretos de bilhões de dólares, devido a investigações, reforço de segurança e custos de mitigação e danos à reputação da SolarWinds, que viu seu software envolvido em um dos ataques cibernéticos mais sofisticados da história.

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

Assinaturas digitais robustas para garantir a integridade das atualizações de software, verificando se o software não foi alterado após a sua criação, monitoramento de comportamento anômalo em redes que utilizam o software Orion, o que poderia detectar acessos não autorizados mais rapidamente e aplicação de patches de segurança rapidamente e revisões periódicas dos softwares utilizados para garantir a detecção de vulnerabilidades conhecidas.