# Ataques Cibernéticos

#### Exercício Aula - 3

Davi Deosmar Batista Oliveira Miranda – RA: 823.212.282  
Silas Rodrigues Nascimento – RA: 823.273.38

# SolarWinds

#### Data do ataque

O ataque teve início em meados de 2020 e foi descoberto em dezembro do mesmo ano.

#### **Tipo de ataque**

O ataque à SolarWinds foi um ataque típico à cadeia de suprimentos. Nesses tipos de hacks, os invasores não buscam diretamente as redes de suas vítimas. Em vez disso, eles penetram no sistema de um fornecedor terceirizado com acesso aos ativos de rede de seus alvos. Nesse caso, o fornecedor terceirizado era a SolarWinds.

#### **Descrição do ataque**

Os hackers infiltraram-se na cadeia de fornecimento da SolarWinds, inseriram código malicioso no software Orion, que é amplamente utilizado por empresas e agências para monitoramento de redes.

* Em setembro de 2019, os hackers puderam acessar a rede SolarWinds.
* Eles começaram a testar sua injeção de código em Orion em outubro de 2019.
* Cerca de quatro meses depois, eles injetaram código malicioso chamado Sunburst no Orion.
* Em 26 de março de 2020, a SolarWinds começou a distribuir atualizações da Orion que continham o código malicioso dos hackers.

O malware se espalhou à medida que milhares de clientes da SolarWinds instalaram o código malicioso na atualização hackeada. Uma vez no sistema de uma vítima, o malware deu aos hackers acesso aos sistemas de TI do cliente.

#### **Vulnerabilidade explorada**

O ataque à SolarWinds de 2020 não se define por um único evento "sem CVE"; em vez disso, foi um ataque sofisticado à cadeia de suprimentos que envolveu a implantação de atualizações de software trojanizadas contendo um backdoor, posteriormente denominado [SUNBURST](https://www.google.com/search?rlz=1C1GCEA_enBR1177BR1177&cs=0&sca_esv=cdd4458fa27f824d&sxsrf=AE3TifPWJQ2G533EopTAGSQrsP7lpo9LDw%3A1757973979989&q=SUNBURST&sa=X&ved=2ahUKEwirtsK049uPAxXjHbkGHXMVIzcQxccNegQIAxAB&mstk=AUtExfDr3ntgR9CVz5n1Hf9ApUFXu9ezKbZyrQjxKBZCbeMqMUfZkfNgXwTRxA0TMJq9MhWdJJ605rK3RGfCM4jW6TRPjZQAsw5rOB9jepBkc5cdIy008NvsmqHTBVKfhfi2cpDIiJyCZCxVRGyhENA23LWSzHE45IZZ8CPgPZDgQoNjOAw&csui=3).

#### Prejuízos

Os prejuízos incluíram: espionagem e roubo de dados em agências governamentais e empresas privadas, como a Microsoft e o Pentágono; exposição de redes de infraestrutura crítica; danos à reputação da SolarWinds; e o endurecimento do mercado de seguros cibernéticos, com aumento de custos e restrições de cobertura para os segurados.

#### Medidas de prevenção

### Para a empresa:

* Avaliação da cadeia de fornecimento
* Implementação de práticas de segurança no desenvolvimento de software
* Monitoramento e detecção avançada de ameaças
* Gerenciamento de vulnerabilidades e patches
* Controle de acesso e privilégios
* Segurança na nuvem
* Treinamento e conscientização dos funcionários

### Para o cliente:

* Manutenção de dispositivos atualizados
* Utilização de software de segurança
* Práticas de segurança online
* Backup regular de dados
* Conscientização de ameaças

# CardersMarket

#### Data do ataque

O “ataque” central relacionado ao CardersMarket não foi um único evento, mas sim uma série de invasões que aconteceram em meados de 2006 até 2007.

#### **Tipo de ataque**

O tipo de ataque usado pelo Max Butler (Iceman) para assumir o controle dos fóruns concorrentes e fortalecer o CardersMarket foi principalmente de natureza invasão a sistemas web e bases de dados.

∙ Ataques de aplicação web (SQL Injection, roubo de credenciais).

∙ Intrusão em servidores (exploits e malware).

∙ Takeover de sistemas rivais (migração e destruição de fóruns concorrentes).

∙ Roubo de dados financeiros (sniffers em redes POS).

#### **Descrição do ataque**

O ataque do CardersMarket (2006–2007) foi conduzido por Max Butler (Iceman).Ele explorou falhas em fóruns rivais de carders (principalmente vulnerabilidades em aplicações web e senhas fracas), roubou os bancos de dados de usuários e os migrou para o seu próprio fórum. Depois, em alguns casos, derrubava os sites originais, forçando os membros a usar o CardersMarket, que chegou a ter milhares de usuários.

Paralelamente, ele também invadia redes de empresas e sistemas de ponto de venda (POS) para roubar dados de cartões de crédito, que eram vendidos em grande escala dentro do fórum.

Em resumo: foi uma combinação de invasão de fóruns concorrentes + roubo de dados financeiros em redes de varejo, consolidando tudo em um único mercado clandestino.

#### **Vulnerabilidade explorada**

o ataque principal usado por Max Butler foi SQL injection contra softwares de fórum — mas não há um único “CVE do CardersMarket”: ele explorou vulnerabilidades em vários fóruns/softwares diferentes. Com base em reportagens e bases de vulnerabilidades, exemplos de CVEs que correspondem ao tipo de falha explorada (SQLi em softwares de fórum na mesma época) são:

**CVE-2006-7071** — SQL injection em Invision Power Board (IPB) 2.1 ≤ 2.1.6. [NVD](https://nvd.nist.gov/vuln/detail/CVE-2006-7071?utm_source=chatgpt.com)

**CVE-2006-3994** — SQL injection em XMB (Extreme Message Board) 1.9.6 alpha e anteriores

#### Prejuízos

O ataque do CardersMarket, liderado por Max Butler resultou no roubo de aproximadamente 1,8 milhão de números de cartões de crédito e débito. As fraudes associadas geraram um prejuízo estimado em 86,4 milhões de dólares, e a Justiça determinou que Butler pagasse 27,5 milhões em restituição às vítimas.

#### Medidas de prevenção

O uso de atualizações e patches regulares em softwares de fórum e servidores teria fechado brechas conhecidas como SQL Injection. A implementação de validação e sanitização de entradas no código das aplicações também impediria a exploração de comandos maliciosos no banco de dados. Além disso, uma política forte de gestão de credenciais, com senhas únicas e autenticação em dois fatores para administradores, teria reduzido o risco de invasores reutilizarem senhas.