Caso 1: Ataque à Kaseya VSA — Comprometimento da Cadeia de Suprimentos

Data: 2 de julho de 2021

Tipo de ataque: Ransomware via cadeia de suprimentos

Autor: Grupo REvil (também conhecido como Sodinokibi)

O que aconteceu:

Uma vulnerabilidade crítica e desconhecida até então (CVE-2021-30116) foi explorada no software de gerenciamento remoto VSA, da empresa Kaseya. Os invasores enviaram uma falsa atualização que disseminou ransomware para centenas de empresas clientes. Estima-se que entre 800 e 1.500 organizações foram afetadas globalmente.

Impacto:

A rede de supermercados Coop, na Suécia, foi uma das vítimas mais notórias — centenas de lojas precisaram ser fechadas. O grupo criminoso exigiu US$ 70 milhões em Bitcoin para liberar uma chave de desbloqueio universal.

? **Estratégias de Defesa:**

- **Para desenvolvedores e fornecedores:**
  - Implementação de práticas de desenvolvimento seguro (Secure SDLC)
  - Revisões regulares de código
  - Testes de intrusão contínuos
- **Para empresas clientes:**
- Segmentação da rede interna
- Aplicação do princípio do menor privilégio
- Backups protegidos e desconectados (offline ou em nuvem)

? Caso 2: Log4Shell — Execução Remota de Código

Data: Dezembro de 2021

Tipo de ataque: Exploração de falha crítica (Remote Code Execution)

Vulnerabilidade: CVE-2021-44228

O que aconteceu:

A falha conhecida como “Log4Shell” afetou a biblioteca Log4j, amplamente utilizada em aplicações Java. Bastava enviar uma string específica para um servidor vulnerável para que o invasor obtivesse controle total do sistema.

Impacto:

O alcance foi global e devastador, afetando desde servidores de jogos como Minecraft até gigantes da nuvem como Amazon AWS e Apple iCloud. O prejuízo foi estimado em bilhões de dólares. A gravidade da falha foi classificada como 10.0 (máxima) no sistema CVSS.

⍰ Estratégias de Defesa:

- **Contenção:** Atualização imediata para Log4j versão 2.15.0 ou superior
- **Prevenção:** Implementação de firewalls de aplicação web (WAF) para bloquear padrões suspeitos
- **Mitigação:** Desativação da função JNDI em sistemas que não puderam ser atualizados