Ataque 1: Caso Kaseya VSA (Ataque à Cadeia de Suprimentos)

- **Data:** 2 de julho de 2021
- **Tipo:** Ataque à Cadeia de Suprimentos com *Ransomware*
- **Responsáveis:** Grupo REvil (Sodinokibi)

O grupo REvil explorou uma falha de "dia zero" (CVE-2021-30116) no software de gerenciamento remoto VSA, da empresa Kaseya. Por meio dessa vulnerabilidade, enviaram uma atualização maliciosa que espalhou ransomware para centenas de empresas que utilizavam o sistema — atingindo indiretamente cerca de **800 a 1.500 organizações** no mundo.

O ataque paralisou operações inteiras, como a rede de supermercados **Coop**, na Suécia, que precisou fechar centenas de lojas. O grupo chegou a exigir **US$ 70 milhões em Bitcoin** por uma chave de descriptografia universal.

Medidas de proteção:

- Para fornecedores: adoção de ciclos de desenvolvimento seguro (Secure SDLC), auditorias de código e testes de penetração constantes.
- Para clientes: segmentação de rede, princípio do menor privilégio e backups imutáveis (offline ou em nuvem).

Ataque 2: Vulnerabilidade Log4Shell (Exploração de Dia Zero)

- **Data:** Dezembro de 2021
- **Tipo:** Exploração de Vulnerabilidade de Dia Zero (*Remote Code Execution*)
- **Vulnerabilidade:** CVE-2021-44228

A falha "Log4Shell" afetou a biblioteca **Log4j**, amplamente usada em aplicações Java. Ela permitia que uma simples string de texto enviada a um servidor vulnerável resultasse na execução remota de código malicioso, concedendo controle total ao invasor.

O impacto foi **global e sem precedentes**, atingindo bilhões de sistemas — de servidores de jogos, como *Minecraft*, até serviços de nuvem como **Amazon AWS** e **Apple iCloud**. O prejuízo estimado chegou a **bilhões de dólares**, e a falha foi avaliada com gravidade **10.0 (Crítico)** no sistema CVSS.

Medidas de proteção:

- **Contenção:** atualização imediata do Log4j para a versão 2.15.0 ou superior.
- **Prevenção:** uso de *Web Application Firewalls* (WAF) para bloquear strings suspeitas.

- **Mitigação:** desativação da função vulnerável (*JNDI lookups*) em sistemas que não puderam ser atualizados de imediato.