Ataque 1: Vulnerabilidade no MOVEit Transfer (svr de transferência de arquivos)

1. **Data aproximada do ataque**
   O problema foi descoberto publicamente em 31 de maio de 2023 e a exploração começou pouco antes dessa data.
2. **Tipo de ataque**
   Trata-se de *vazamento / exfiltração massiva de dados* via exploração de vulnerabilidade de software (ataque à cadeia de transferência de arquivos usada por muitas organizações).
3. **Descrição de como aconteceu**
   A vulnerabilidade permitia que um atacante não autenticado fizesse **injeção de SQL** no aplicativo MOVEit Transfer, obtendo acesso ao banco de dados da aplicação, podendo modificar ou excluir conteúdos, podendo depois instalar web-shells e extrair dados armazenados.
   O grupo de ransomware Cl0p ("Clop") aproveitou-se dessa falha para atingir milhares de organizações em diversos setores, exfiltrando dados sensíveis (pessoal, bancário) e exigindo pagamento.
4. **Vulnerabilidade explorada (CVE)**
   - Uma das principais CVEs: CVE-2023-34362 — injeção de SQL não autenticada no MOVEit Transfer.
   - Outras relacionadas: CVE-2023-35036 e CVE-2023-35708 também vieram à tona nas correções subsequentes.
5. **Impactos e/ou prejuízo (estimado)**
   - Estima-se que mais de **2.700 organizações** tenham sido afetadas.
   - Aproximadamente **93 milhões de registros pessoais** foram comprometidos.
   - Impacto setorial amplo: governo, saúde, financeiro, serviços. Além de custo de resposta, multas, danos à reputação, extorsão de dados.
6. **Tipo de Proteção que poderia ter sido aplicada para evitá-lo**
   - **Patch e atualização imediata** da solução MOVEit com as correções de segurança assim que foram disponibilizadas.
   - **Restrição de acesso externo** (por exemplo, bloquear/travar HTTP/HTTPS públicos para a aplicação enquanto a correção era aplicada).
   - **Monitoramento e detecção de anomalias**: logs de acesso, alertas de uso de web-shells ou padrões estranhos de banco de dados.
   - **Aplicação de boas práticas de desenvolvimento seguro**: por exemplo, defender contra injeção de SQL (validação de entrada, prepared statements), minimização dos privilégios da aplicação no banco de dados.
   - **Backup e segregação de dados sensíveis**, de modo que mesmo se exfiltrados, o impacto seja menor.

Ataque 2: Vulnerabilidade no Citrix NetScaler ADC & Gateway (dispositivo de entrega de aplicações / acesso remoto)

1. **Data aproximada do ataque**
   A vulnerabilidade foi divulgada em 10 de outubro de 2023, e a exploração ativa (zero-day) foi identificada já em agosto-setembro de 2023.
2. **Tipo de ataque**
   É um ataque de *divulgação de informação / sequestro de sessão (session hijacking)* em dispositivos de acesso corporativo, que pode levar à execução subsequente de intrusão mais profunda ou ransomware.
3. **Descrição de como aconteceu**
   A vulnerabilidade, conhecida como CVE-2023-4966, permitia que um atacante não autenticado realizasse uma requisição HTTP especialmente construída ao dispositivo NetScaler Gateway/ADC vulnerável, resultando numa *leitura de memória* ou exposição de tokens de sessão, credenciais ou dados de autenticação, com possibilidade de sessão válida ser tomada pelo invasor.
   O exploit foi usado por grupos de ransomware como o LockBit para obter controle ou acesso privilegiado via o dispositivo vulnerável.
4. **Vulnerabilidade explorada (CVE)**
   A vulnerabilidade principal é CVE-2023-4966.
   (Outras relacionadas: CVE-2023-4967 etc.)
5. **Impactos e/ou prejuízo (estimado)**
   - A vulnerabilidade foi utilizada para "session hijacking" em múltiplas organizações, podendo levar ao comprometimento de acesso VPN/remote.
   - Por exemplo, a empresa Comcast divulgou que cerca de 35 milhões de contas Xfinity foram afetadas via essa vulnerabilidade.
   - O impacto inclui acesso não autorizado, possível implantação de ransomware, interrupção de serviços, custo de contenção, comunicação de violação, perda de confiança.
6. **Tipo de Proteção que poderia ter sido aplicada para evitá-lo**
   - **Atualização imediata do firmware/software** do appliance Citrix NetScaler para versão corrigida.
   - **Redução da exposição externa** desses dispositivos: limitar acesso direto à Internet, usar rede de perímetro, segmentação de rede, bastion hosts.
   - **Autenticação forte e monitoramento de sessões**: detectar sessões atípicas, logs de criação/uso de tokens, invalidação de sessões ativas após correção.
   - **Segurança de perímetro fortalecida**: firewall, WAF, IDS/IPS que identifiquem requisições mal-formadas ou tentativas de exploração de memória.
   - **Backups e teste de recuperação** para mitigar o impacto caso ransomware ou acesso privilegiado ocorra.