**SCS: Proteção de dados e informações**

**Prof. Robson Calvetti**

*Juliana Gomes – Otavio Teles de Sousa*

**Ataque 1. Ataque ao sistema Colonial Pipeline.**

O ataque ao sistema da empresa Colonial Pipeline ocorreu em maio de 2021, sendo um dos incidentes cibernéticos mais impactantes nos Estados Unidos nos últimos cinco anos. O ataque iniciou-se em torno do dia 7 de maio de 2021, quando os hackers conseguiram acesso remoto à rede da Colonial Pipeline, que é responsável pelo maior oleoduto de combustíveis dos EUA. O tipo de ataque foi um ransomware, que criptografou sistemas essenciais da empresa e provocou a interrupção parcial das operações do oleoduto. Os invasores utilizaram um vírus de resgate para bloquear o acesso aos dados, exigindo pagamento em criptomoedas para liberar o sistema.

O ataque aconteceu após a invasão inicial obtida por meio do comprometimento de uma credencial de acesso VPN que não tinha autenticação multifator ativada, o que permitiu o acesso remoto sem uma camada adicional de segurança. Com essa brecha, os hackers entraram na rede interna da Colonial Pipeline e implantaram o ransomware denominado DarkSide. A infecção se espalhou rapidamente pelos sistemas da empresa, causando a paralisação das operações e provocando escassez de combustível em vários estados do país, além de aumento dos preços. A empresa acabou pagando um resgate de cerca de 4,4 milhões de dólares para recuperar o acesso aos sistemas.

A vulnerabilidade explorada, embora não esteja ligada a um CVE específico por ser mais uma falha na política de segurança (falta de autenticação multifator e proteção adequada das credenciais), pode ser relacionada a práticas inadequadas de gerenciamento de acesso e credenciais, que são as maiores portas de entrada para ataques do tipo ransomware. O ponto crítico foi o acesso VPN desprotegido, o que é uma falha operacional mais do que técnica, mas que abriu caminho para a exploração maliciosa.

Os impactos foram severos. Além do pagamento do resgate, o ataque gerou interrupções significativas no fornecimento de combustível para a costa leste dos EUA, levando a desabastecimento, aumento dos preços e impacto econômico regional. Também provocou danos à reputação da empresa e gerou preocupação nacional quanto à segurança de infraestruturas críticas. O custo total do incidente, incluindo resposta, recuperação, mitigação e impacto econômico indireto, é estimado em dezenas de milhões de dólares.

Quanto às proteções que poderiam ter evitado ou mitigado o ataque, destacam-se:

* Implementação obrigatória de autenticação multifator (MFA) para todos os acessos remotos;
* Políticas rigorosas de gerenciamento e rotação de credenciais;
* Segmentação da rede para limitar a propagação do ransomware;
* Treinamento constante dos funcionários sobre segurança da informação;
* Manutenção de backups atualizados e isolados para rápida recuperação;
* Testes de penetração e auditorias regulares para identificar vulnerabilidades;
* Uso de soluções anti-malware e sistemas de detecção/prevenção de intrusão.

**Ataque 2. Ataque MOVEit Transfer**

O ataque ao MOVEit Transfer ocorreu no final de maio de 2023, com as primeiras explorações detectadas entre os dias 27 e 31 de maio. Essa vulnerabilidade foi explorada por um grupo conhecido como Cl0p, que utiliza ataques de ransomware combinados com vazamento de dados para chantagear as vítimas. O tipo de ataque caracterizou-se como uma exploração remota e não autenticada de vulnerabilidade crítica de SQL Injection (SQLi), permitindo aos invasores manipularem diretamente o banco de dados do MOVEit Transfer via requisições HTTP maliciosas. Por meio dessa brecha, os hackers conseguiram inserir uma web shell, denominado “LemurLoot”, que lhes concedeu controle remoto sobre os servidores comprometidos. Com esse acesso, foi possível executar comandos arbitrários, acessar, copiar e extrair dados sensíveis armazenados nas instâncias vulneráveis do MOVEit. A Progress Software, empresa responsável pelo software, lançou rapidamente patches emergenciais para corrigir essa falha e recomendou medidas de mitigação.

A vulnerabilidade explorada recebeu o código CVE-2023-34362 e está classificada como uma falha crítica de segurança. Essa falha permitia que invasores não autenticados executassem comandos SQL maliciosos, abrindo caminho para acesso remoto e execução de código arbitrário no servidor afetado. Posteriormente, outras vulnerabilidades relacionadas também foram corrigidas, como a CVE-2023-35036 e a CVE-2023-35708, ambas relacionadas a problemas adicionais de segurança no MOVEit Transfer, todas envolvendo falhas em tratamento inadequado de entradas, o que possibilitava injeções de código.

Quanto aos impactos, estimativas indicam que centenas de organizações ao redor do mundo foram afetadas, incluindo empresas do setor financeiro, órgãos governamentais, instituições de saúde e outras entidades sensíveis. Os dados extrair incluíam informações pessoais, documentos financeiros, contratos, dados de clientes e funcionários, além de outras informações confidenciais e estratégicas. Os prejuízos financeiros foram significativos, contemplando custos com resposta a incidentes, investigações forenses, remediação, possíveis multas regulatórias relacionadas a leis de proteção de dados como GDPR e LGPD, além do impacto na reputação das organizações envolvidas, com perdas na confiança de clientes e parceiros. Ademais, o vazamento dos dados possibilitou riscos adicionais, como fraudes, roubo de identidade e espionagem corporativa. O tempo até a detecção e mitigação do ataque em alguns casos chegou a dias ou semanas, o que agravou os efeitos.

Quanto ao tipo de proteção que poderia ter evitado esse ataque, algumas medidas fundamentais são:

* Aplicação rápida e sistemática de patches para corrigir vulnerabilidades conhecidas;
* Implementação de firewall de aplicação web (WAF) para bloquear requisições maliciosas;
* Validação e sanitização rigorosa das entradas na aplicação para prevenir injeções SQL;
* Planos de resposta a incidentes e treinamento da equipe para reação rápida;
* Backup frequente e seguro dos dados para garantir recuperação em caso de ataque.