**Universidade São Judas Tadeu**

**Sistemas Computacionais e Segurança**

**Prof° Robson Calvetti**

Lucas Gabriel Hora Benetti - 825134041

### **Ataque à JBS**

1. Data do ataque: Maio de 2021.
2. Tipo de ataque: Ransomware.
3. Descrição do ataque: O ataque foi conduzido pelo grupo de cibercriminosos REvil. Eles invadiram a rede da JBS e criptografaram seus sistemas de produção e arquivos críticos. Para liberar os dados e restaurar as operações, os hackers exigiram um resgate em criptomoeda. A JBS pagou US$ 11 milhões em Bitcoin para recuperar o controle.
4. Vulnerabilidade explorada: A JBS não divulgou a vulnerabilidade específica. No entanto, a maioria dos ataques de ransomware desse tipo começa com a exploração de sistemas mal gerenciados, como acesso remoto (RDP) desprotegido ou falhas em softwares de VPN para os quais as empresas não aplicaram patches de segurança. Não há uma CVE pública associada diretamente a este ataque.
5. Impactos e/ou prejuízo: O ataque paralisou a produção de carne em várias unidades da empresa nos Estados Unidos, Canadá e Austrália, causando uma interrupção significativa na cadeia de suprimentos de alimentos global. O prejuízo direto incluiu o pagamento do resgate de US$ 11 milhões, além dos custos operacionais e de reputação.
6. Tipo de proteção que poderia ter sido aplicada:
   * Backups isolados: Manter cópias de segurança de dados em um ambiente offline, inacessível aos hackers, permitiria à JBS restaurar seus sistemas sem ter que pagar o resgate.
   * Autenticação Multifator (MFA): Exigir a MFA para todos os acessos remotos e sistemas críticos poderia ter impedido que os hackers acessassem a rede mesmo se tivessem obtido as credenciais de login.

### 

### 

### **Ataque à Snowflake**

1. Data do ataque: Maio a Junho de 2024.
2. Tipo de ataque: Roubo de credenciais (Data Exfiltration).
3. Descrição do ataque: Cibercriminosos invadiram contas de clientes da Snowflake, como Ticketmaster e o Banco Santander, utilizando credenciais de login que haviam sido roubadas de malwares ladrões de informação, que haviam infectado as máquinas de funcionários das empresas afetadas. Os hackers não exploraram uma falha na plataforma da Snowflake, mas sim a falta de segurança por parte dos clientes.
4. Vulnerabilidade explorada: Não houve uma vulnerabilidade técnica na própria plataforma Snowflake (nenhuma CVE foi emitida). A falha explorada foi a falta de Autenticação Multifator (MFA) e o uso de senhas fracas ou reutilizadas por parte dos clientes.
5. Impactos e/ou prejuízo: O ataque resultou no vazamento de informações sensíveis de milhões de usuários. No caso da Ticketmaster, os dados roubados incluíram nomes, endereços, números de telefone e detalhes de cartões de crédito. Os dados foram publicados em fóruns de cibercrime, causando um impacto global na reputação e na confiança do cliente.
6. Tipo de proteção que poderia ter sido aplicada:
   * Autenticação Multifator (MFA): A medida mais eficaz. A MFA impede que os hackers acessem uma conta mesmo que tenham a senha, pois eles precisariam de um segundo fator de autenticação.
   * Monitoramento de acesso: Ferramentas que analisam padrões de comportamento de usuários poderiam ter detectado e alertado sobre acessos incomuns ou a partir de locais atípicos.