Victor Domingos Moreira - 825155879

Felipe Duarte Battaglini - 825165863

Cauã Guidio Viana - 825168423

Lucas Gonçalves da Silva-825113362

Victor de Morais Nelson 825243925

Vietnam investiga ataque cibernético a dados de credores

Data do Ataque: O ataque foi descoberto e noticiado por volta do dia **12 de setembro de 2025**.

Tipo de Ataque: Este é um ataque de **roubo de dados** ou **vazamento de dados**. O objetivo dos hackers era obter acesso não autorizado para roubar informações pessoais e financeiras de uma grande base de dados.

Descrição do Ataque: O ataque teve como alvo o **Centro Nacional de Informação de Crédito (CIC)** do Vietnã, uma unidade ligada ao Banco Estatal do Vietnã. O CIC armazena dados confidenciais de credores, como informações pessoais, histórico de pagamentos de crédito e dados de cartão de crédito. Uma investigação inicial apontou que houve um acesso não autorizado com a intenção de roubar esses dados. As autoridades suspeitam que o ataque foi orquestrado pelo grupo internacional de hackers **Shiny Hunters.**

Vulnerabilidade Explorada: A reportagem não especifica a vulnerabilidade técnica exata (como um código CVE) que foi explorada. No entanto, o sucesso do ataque sugere que havia uma falha de segurança na infraestrutura de TI do CIC, possivelmente uma **configuração incorreta**, um **acesso privilegiado exposto** ou um **software desatualizado** que permitiu que os hackers do Shiny Hunters tivessem acesso à base de dados.

Impactos e/ou Prejuízos:

- **Vazamento de dados confidenciais:** O principal impacto foi o roubo de uma grande quantidade de dados sensíveis de credores. O número exato de contas afetadas não foi divulgado.
- **Aumento de custos para bancos:** O banco de investimento JPMorgan comentou que o incidente poderia levar a um aumento nos custos para os bancos vietnamitas, que precisariam investir mais em segurança cibernética.
- **Potencial risco para depósitos:** Embora o sistema do CIC não tenha sido interrompido, o vazamento de dados gerou um risco potencial para os depósitos bancários e a confiança do público.

Tipo de Proteção que Poderia Ter Sido Usada para Evitá-lo:

- **Criptografia de Dados:** Criptografar os dados sensíveis, tanto em repouso (na base de dados) quanto em trânsito, tornaria as informações roubadas inúteis para os hackers.
- **Controle de Acesso Rigoroso:** Implementar o princípio do "menor privilégio", onde os usuários (ou sistemas) só têm acesso aos dados e recursos estritamente necessários para suas funções, dificultaria a movimentação lateral dos hackers.
- **Monitoramento de Segurança:** Ferramentas de SIEM (Gerenciamento de Eventos e Informações de Segurança) poderiam detectar atividades suspeitas em tempo real, alertando a equipe de segurança sobre o acesso não autorizado antes que o roubo de dados fosse concluído.
- **Autenticação Multifator (MFA):** Exigir um segundo fator de autenticação para acessos críticos, especialmente para administradores de sistema, adicionaria uma camada extra de proteção.
- **Auditorias de Segurança Periódicas:** Realizar auditorias e testes de penetração regulares para identificar e corrigir vulnerabilidades antes que os criminosos possam explorá-las.

Funcionário recebe US$ 920 por credenciais usadas em assalto a banco de US$ 140 milhões

Data do Ataque: O ataque ocorreu em **30 de junho de 2025**. O funcionário foi preso em 3 de julho.

Tipo de Ataque: Este foi um ataque de **ameaça interna (insider threat)** combinado com **engenharia social**. Os criminosos não exploraram uma falha técnica no sistema da empresa C&M, mas sim manipularam e subornaram um funcionário para obter acesso e realizar as ações maliciosas.

Descrição do Ataque: Hackers roubaram quase **$140 milhões de seis bancos brasileiros**. Eles não invadiram os sistemas diretamente, mas usaram as credenciais de um funcionário da **C&M**, uma empresa que fornece soluções de conectividade financeira. Os criminosos subornaram o funcionário, **João Nazareno Roque**, por cerca de $920 para que ele lhes fornecesse suas credenciais corporativas e executasse comandos em um sistema confidencial conectado ao Banco Central do Brasil. Roque seguiu as instruções dos hackers e recebeu um segundo pagamento de $1.850. O funcionário foi preso três dias depois do ataque, e a polícia brasileira está investigando o caso, mas os detalhes sobre os hackers não foram divulgados.

Vulnerabilidade Explorada: A vulnerabilidade principal explorada foi a **fraqueza humana**. O ataque não se baseou em uma falha de software ou configuração (não há um código CVE associado), mas sim na **falta de ética** e **vulnerabilidade do funcionário** à engenharia social e suborno. A empresa C&M afirmou que o ataque só foi possível por meio de engenharia social, e não por uma falha de segurança em seus sistemas.

Impactos e/ou Prejuízos:

- **Prejuízo financeiro direto:** O roubo de quase $140 milhões dos bancos envolvidos.
- **Conversão em criptomoedas:** Uma parte do dinheiro roubado (entre $30 e $40 milhões) já foi convertida em criptomoedas como BTC, ETH e USDT, dificultando o rastreamento e a recuperação.

- **Perda de reputação:** Os bancos e a empresa C&M sofrem com a perda de confiança e credibilidade junto a seus clientes e parceiros.

Tipo de Proteção que Poderia Ter Sido Usada para Evitá-lo:

- **Princípio do Menor Privilégio:** Limitar o acesso do funcionário apenas ao que é estritamente necessário para o seu trabalho, impedindo que ele pudesse executar comandos críticos para a fraude.
- **Monitoramento de Comportamento de Usuário (UEBA):** Ferramentas de UEBA poderiam ter detectado atividades anômalas, como comandos fora do padrão ou o acesso em horários incomuns, levantando um alerta para a equipe de segurança.
- **Autenticação Multifator (MFA) Obrigatória:** Mesmo com o suborno das credenciais, o MFA exigiria um segundo fator de autenticação (como um código enviado para o celular do funcionário) para confirmar o login, tornando a operação mais difícil para os hackers.
- **Treinamento de Conscientização:** Treinamento contínuo sobre engenharia social, ameaças de insider e a importância de relatar qualquer abordagem suspeita poderia ter ajudado o funcionário a não ceder ao suborno.
- **Segregação de Funções:** Dividir as tarefas críticas entre vários funcionários para que um único indivíduo não possa causar um dano massivo sozinho.

Referências:

artigo 1

https://www.reuters.com/sustainability/boards-policy-regulation/vietnam-investigates-cyberattack-creditors-data-2025-09-12/?utm_source

artigo 2

https://www.bleepingcomputer.com/news/security/employee-gets-920-for-credentials-used-in-140-million-bank-heist/?utm_source=chatgpt.com