Trabalho – Ataques Cibernéticos no Brasil

# Ataque ao SIAFI / gov.br (2024)

**Data aproximada :** Abril de 2024

**Tipo de Ataque:** Phishing + uso de credenciais roubadas + fraude financeira

**Como aconteceu:**Hackers obtiveram senhas e certificados digitais de servidores do governo, acessaram o sistema SIAFI e autorizaram transferências bancárias irregulares.

Com essas credenciais e certificados, fizeram alterações nas ordens bancárias ou pré-docs, desviando valores para destinatários que não eram os legítimos.

**Vulnerabilidade Exploradas:**Falha na segurança de acesso (não há CVE divulgado).

A vulnerabilidade principal parece estar na segurança do acesso, e autenticação (certificado digital fraudado) ou seja, falha operacional / de processo e talvez falhas de validação de certificado digital.

**Impactos / Prejuízos:**Desvio de cerca de R$ 15 milhões e mais de 200 tentativas de fraudes detectadas e bloqueadas.

**Proteção que Poderia Ter Evitado:**Autenticação multifator, controle mais rígido na emissão de certificados digitais, monitoramento de acessos e treinamento contra phishing.

Monitoramento e alertas de uso indevido de credenciais, logs de acesso, detecção de padrões anômalos (por exemplo, acesso de localização ou horário estranho).

# 2. Vazamento de Dados da Netshoes (2024)

**Data aproximada:** Julho de 2024

**Tipo de Ataque: v**azamento de dados pessoais / incidente de segurança / exposição de dados de clientes.

**Como aconteceu:** Dados de aproximadamente 38 milhões de usuários foram expostos, incluindo CPF, endereço e histórico de compras. O hacker publicou tudo em fórum de cibercrime. Foram expostos registros de compras de 40 milhões, contendo informações como Nome, endereço, telefone, datas de pedido, número de pedidos, Documentos e fornecedores terceirizados.

**Vulnerabilidade Exploradas:** Não foi publicamente divulgado um CVE específico para esse incidente, nem a técnica específica de invasão. se foi SQL injection, falha de configuração ou acesso indevido.

**Impactos / Prejuízos: Grande número de usuários afetados, dados pessoais expostos que poderiam elevar a golpes.**

**Proteção que Poderia Ter Evitado:**Criptografia de dados, auditorias de segurança frequentes, revisão de permissões de acesso e políticas de retenção de dados.

Menor exposição de dados pessoais em sistemas públicos ou de terceiros.

Políticas de retenção de dados: guardar só o necessário, e por tempo que seja legalmente ou operacionalmente exigido, eliminando o que não for necessário para diminuir a superfície de ataque.