# Relatório de Incidente de Segurança

## Seção 1: Identificar o protocolo de rede envolvido no incidente

Durante a investigação do incidente de segurança no site yummyrecipesforme.com, foram identificados os seguintes protocolos de rede usados:  
  
- DNS (Domain Name System): para resolução de nomes de domínio.  
- HTTP (Hypertext Transfer Protocol): usado para solicitar e carregar páginas web.  
- TCP (Transmission Control Protocol): protocolo de transporte usado na comunicação entre cliente e servidor.  
- JavaScript (embutido no código-fonte): utilizado para acionar o download automático de arquivos.

## Seção 2: Documentar o incidente

O site da empresa foi comprometido após um ataque de força bruta realizado por um ex-funcionário. O atacante utilizou senhas padrão conhecidas para acessar o painel de administração. Após obter acesso, ele:  
  
1. Incorporou um script JavaScript malicioso ao código-fonte do site.  
2. O script forçava os visitantes a baixarem e executarem um arquivo supostamente necessário para "atualizar o navegador".  
3. Esse arquivo redirecionava os usuários automaticamente para outro domínio (greatrecipesforme.com) que continha malware.  
4. O atacante também alterou a senha da conta administrativa, impedindo o acesso do proprietário do site.  
  
Clientes relataram lentidão nos computadores e redirecionamento suspeito após a execução do arquivo. A análise do tráfego via tcpdump confirmou que, após o acesso ao site original, ocorriam resoluções DNS e conexões HTTP com o site malicioso.  
  
O ataque foi descoberto após o proprietário do site relatar problemas de acesso e clientes reclamarem por e-mail. A equipe de segurança criou um ambiente sandbox, reproduziu o problema e confirmou a presença do malware e do redirecionamento.

## Seção 3: Recomendação para evitar ataques de força bruta

Recomenda-se a implementação de autenticação de dois fatores (2FA) para todas as contas administrativas do site. Isso adiciona uma camada extra de segurança, exigindo não apenas uma senha, mas também um segundo fator (como um código enviado ao celular). Mesmo que uma senha seja descoberta, o acesso não será possível sem esse segundo fator.  
  
Outras boas práticas incluem:  
- Impor senhas fortes e não padrão  
- Limitar tentativas de login por IP  
- Monitorar e registrar tentativas de login suspeitas  
- Desativar contas inativas ou de ex-funcionários