# Relatório de incidente de segurança

|  |
| --- |
| **Section 1: Identifique o protocolo de rede envolvido no incidente** |
| O incidente envolve os protocolos de rede DNS e HTTP, essenciais para a comunicação e resolução de endereços IP associados aos domínios acessados. O protocolo DNS foi usado para resolver o endereço IP de ambos os sites envolvidos no incidente: yummyrecipesforme.com e o site falso greatrecipesforme.com. Após a resolução do endereço IP do site legítimo, o protocolo HTTP foi empregado para carregar o conteúdo da página web. Esse conteúdo incluía um script malicioso que redirecionava os usuários para o site malicioso através de uma nova solicitação DNS, resultando em um download de malware disfarçado alegando que ele forneceria acesso a receitas gratuitas. |
|

|  |
| --- |
| **Section 2: Documentar o incidente** |
| Após um ataque de força bruta bem-sucedido, o ex-funcionário obteve acesso ao painel administrativo do site. O atacante explorou a vulnerabilidade de uma senha padrão ainda ativa e, sem proteção adicional contra tentativas de login excessivas, conseguiu acessar a conta administrativa. Com o controle do painel, o atacante inseriu um código JavaScript malicioso no código-fonte do site yummyrecipesforme.com. Este código solicita que os visitantes baixem um arquivo alegando que ele forneceria acesso a receitas gratuitas. Ao fazer o download, os usuários são redirecionados para greatrecipesforme.com, uma versão falsa do site, que contém o malware.  Após o incidente, os clientes relataram problemas de desempenho em seus dispositivos e receberam mensagens incomuns solicitando o download de arquivos. Quando o proprietário do site tentou acessar o painel de administração para investigar, constatou que a senha havia sido alterada, bloqueando o acesso. Uma análise posterior confirmou que o site havia sido comprometido e o código malicioso estava ativo. |

|  |
| --- |
| **Section 3: Recomendar uma correção para ataques de força bruta** |
| Para prevenir ataques de força bruta no futuro, as seguintes medidas de segurança são recomendadas:   1. Implementação de Autenticação Multifator (MFA): Adicionar MFA para todas as contas administrativas, exigindo um segundo fator de autenticação além da senha. 2. Política de Senhas Fortes: Garantir que todas as senhas de contas administrativas estejam de acordo com as melhores práticas de segurança, exigindo uma combinação de caracteres especiais, números, e um comprimento mínimo de 12 caracteres. Evitar senhas padrão e desativar contas com credenciais padrão. 3. Limitação de Tentativas de Login e Bloqueio Temporário: Configurar o sistema para bloquear temporariamente a conta após um número específico de tentativas falhas, dificultando ataques de força bruta 4. Monitoramento e Alertas de Segurança: Implementar sistemas de monitoramento que enviem alertas ao identificar atividades incomuns, como múltiplas tentativas de login falhas em curto espaço de tempo 5. Proibir o uso de senhas anteriores: Como a vulnerabilidade que levou a esse ataque foi a capacidade do invasor de usar uma senha padrão para fazer login, é importante impedir que senhas antigas, como senhas padrão, sejam usadas para redefinir a senha. |