# Relatório de Incidente de Cibersegurança

| Seção 1: Identifique o protocolo de rede envolvido no incidente |
| --- |
| O **DNS (Domain Name System)** foi usado para descobrir o endereço IP dos sites, primeiro para "yummyrecipesforme.com" e, depois, para o site malicioso "greatrecipesforme.com". O **TCP (Transmission Control Protocol)** foi utilizado para criar a conexão de rede estável entre o usuário e o servidor web. A prova está nos logs com as flags [S] e [S.], que iniciam a conexão. O **HTTP (Hypertext Transfer Protocol)** foi usado para solicitar e carregar o conteúdo das páginas web. Foi através do HTTP que o site comprometido entregou o script malicioso ao usuário. |

| Seção 2: Documente o incidente |
| --- |
| 1. O usuário se conectou ao site "yummyrecipesforme.com". Os logs mostram a consulta DNS e a conexão HTTP inicial.<br>2. Ao carregar o site, um script injetado pelo atacante solicitou o download de um arquivo.<br>3. O script forçou o navegador a fazer uma nova consulta DNS, desta vez para "greatrecipesforme.com". Essa é a prova-chave do redirecionamento.<br>4. O navegador do usuário se conectou ao novo endereço IP, completando o ataque e expondo a máquina ao malware.<br>5. O incidente foi possível porque o atacante obteve acesso ao painel de administração através de um ataque de força bruta, explorando uma senha padrão que nunca foi alterada. |

| Seção 3: Recomende uma solução para ataques de força bruta |
| --- |
| A recomendação principal é implementar uma política de controle de acesso robusta, como políticas de senhas fortes, exigindo senhas com no mínimo 12 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos. Proibir senhas padrão ou fracas. Implementar o bloqueio de conta automático após um número baixo de tentativas de login falhas (ex: 5 tentativas) para neutralizar ataques de força bruta automatizados. Habilitar a Autenticação Multifator (MFA) para todas as contas administrativas. |