Relatório de Incidente de Segurança

Seção 1: Identificar o protocolo de rede envolvido no incidente
Durante a análise do tráfego de rede capturado com `tcpdump`, os seguintes protocolos de rede foram identificados: • **DNS (Domain Name System)**: usado para resolver os domínios `yummyrecipesforme.com` e `greatrecipesforme.com` para seus respectivos endereços IP. • **HTTP (Hypertext Transfer Protocol)**: usado para solicitar e transferir as páginas da web e arquivos, incluindo o malware. • **TCP (Transmission Control Protocol)**: protocolo de transporte usado para estabelecer e manter conexões de rede confiáveis entre cliente e servidor. Esses protocolos operam principalmente nas camadas de aplicação (DNS, HTTP) e de transporte (TCP) do modelo TCP/IP.

Seção 2: Documentar o incidente
Em 5 de junho de 2025, a equipe de segurança da yummyrecipesforme.com foi alertada por clientes que relataram comportamentos suspeitos ao visitar o site. Os visitantes afirmaram que, ao acessar a página principal, foram solicitados a baixar um arquivo supostamente necessário para visualizar receitas gratuitas. Após executar o arquivo, seus navegadores foram redirecionados automaticamente para o site `greatrecipesforme.com`, que apresentou lentidão no sistema dos usuários. ### Investigação Técnica: A equipe criou um ambiente de sandbox e capturou o tráfego de rede com

`tcpdump` durante o carregamento do site. O fluxo observado foi:

1. Requisição DNS para `yummyrecipesforme.com`, resolvendo para o IP `203.0.113.22`.
2. Requisição HTTP para carregar a página.
3. O navegador solicita e baixa um arquivo executável malicioso.
4. Nova requisição DNS para `greatrecipesforme.com`, resolvendo para `192.0.2.17`.
5. Redirecionamento do navegador e conexão HTTP com o novo domínio.

Um analista sênior revisou o código-fonte do site e encontrou um **script JavaScript malicioso** que promovia o download do malware. O script havia sido adicionado após um **ataque de força bruta**, no qual o invasor adivinhou a senha da conta administrativa (que ainda era a senha padrão). O invasor então obteve controle do painel de administração e alterou a senha para impedir a recuperação da conta.

Esse tipo de ataque foi possível devido à **ausência de mecanismos de defesa contra força bruta**, como bloqueio de tentativas ou autenticação adicional.

Seção 3: Recomendar uma medida de mitigação para ataques de força bruta

Recomendação: Implementar **Autenticação de Dois Fatores (2FA)** para todas as contas administrativas.

Justificativa:
A autenticação de dois fatores (2FA) adiciona uma camada essencial de segurança. Mesmo que um invasor descubra a senha de um administrador, ele não poderá acessar o sistema sem o segundo fator (como um código temporário gerado por aplicativo ou enviado por SMS). Isso reduz drasticamente o risco de acesso não autorizado, especialmente quando senhas fracas ou padrão estão em uso.

Medidas Adicionais Recomendadas:

- **Exigir senhas fortes** e exclusivas.
- **Bloquear ou atrasar tentativas após várias falhas de login.**
- **Monitorar e registrar tentativas de login suspeitas.**

- **Forçar mudanças regulares de senha e proibir reutilização.**
- **Realizar auditorias periódicas de segurança.**