Security incident report

Section 1: Identify the network protocol involved in the incident
O protocolo de rede envolvido no incidente é o HTTP, utilizado de forma maliciosa pelo atacante. Isso porque, ao acessar o site *yummyrecipesforme.com* por meio da requisição ao seu servidor web, muito tráfego de rede é recebido e logo em seguida o computador solicitante envia uma nova requisição DNS para encontrar o endereço de outro site, o *greatrecipesforme.com*, e acessá-lo, sem um pedido manual desse acesso por parte do usuário, indicando que foi o payload do HTTP que levou a essa outra requisição.

Section 2: Document the incident
Vários clientes enviaram um e-mail para o helpdesk da yummyrecipesforme relatando que o site da empresa solicitava o download de um arquivo que, depois que era executado, os redirecionava para outro site e deixava o computador lento. O proprietário do site, para verificar o que tinha acontecido, tentou fazer login no painel de administração, mas não conseguiu, e por isso entrou em contato com o provedor de hospedagem. Para entender o que havia acontecido, o analista da equipe de segurança responsável pelo caso criou um ambiente sandbox para entrar no site e analisar o que acontece no tráfego de rede por meio do tcpdump. Ele executou os mesmos passos que os usuários relataram, começando por acessar o site normalmente. Como esperado, foi solicitado o download de um arquivo que supostamente continha receitas gratuitas, e quando esse arquivo foi executado, o analista foi redirecionado do site no qual estava (*yummyrecipesforme.com*) para um outro site (*greatrecipesforme.com)*. Após alguns testes de uso do computador, ele notou que estava lento. A análise do log obtido pelo tcpdump mostrou que até o acesso inicial ao site, tudo ocorria normalmente, mas após a execução do arquivo, o computador do usuário fazia uma consulta DNS para o novo site e o redirecionava para ele. Após uma análise do código fonte do site original e do arquivo, foi identificado

que um trecho do código javascript do site pedia o download deste último, enquanto que o arquivo continha código malicioso para levar o usuário a um site diferente que continha malware.

Como o proprietário do site não conseguiu acessar o painel de administração, é provável que o atacante tenha conseguido a senha de alguma forma e alterado o código fonte do site original para implementar esse ataque, e depois trocado a senha para que o problema não seja resolvido com facilidade.

Section 3: Recommend one remediation for brute force attacks
Dado que o atacante pode ter descoberto a senha pela técnica de força bruta, há várias medidas que poderiam ter prevenido esse ataque. ● Uso de uma senha forte – é essencial trocar a senha padrão para uma senha que não é facilmente descoberta por um ataque de força bruta (que testa várias combinações ou senhas padrão até que encontre uma que funcione). ● Máximo de tentativas – o estabelecimento de um limite de tentativas em um período de tempo impede que um atacante teste muitas senhas de uma vez, o que também dá tempo para que a equipe de segurança perceba a movimentação estranha. ● Autenticação multifator – é preciso que o usuário configure duas formas de garantir que é autêntico, podendo a primeira ser a senha e a segunda uma confirmação por e-mail ou número de telefone, uma pergunta de segurança, entre outras opções.