# Relatório de incidente de cibersegurança

|  |
| --- |
| **Sessão 1: Identifique o protocolo de rede envolvido no incidente** |
| Após alteração no código fonte do site *yummyrecipesforme.com* um código javascript foi adicionado, que utilizando o método **HTTP : GET** através do protocolo **HTTP**, solicita aos visitantes fazer o download de um arquivo malicioso, que após executado os redireciona para outro endereço URL de um site clone. |
|

|  |
| --- |
| **Sessão 2: Documente o incidente** |
| Vários clientes do site *yummyrecipesforme.com* entraram em contato com o suporte técnico da empresa informando que ao acessar seu site foram solicitados a baixar um arquivo que supostamente atualizaria seus navegadores, em seguida relataram ser redirecionados a outro site parecido, mas com o endereço diferente e com os mesmos produtos ofertados no site original sendo disponibilizados gratuitamente, além disso, seus computadores passaram a operar lentamente desde então. Em resposta, o proprietário tentou acessar o painel de administração do site, mas não obteve êxito, foi então que entrou em contato com nossa empresa para investigarmos o incidente.  Um ambiente sandbox foi criado para a investigação, a ferramenta **tcpdump** foi utilizada para criar um log de tráfego DNS & HTTP para analisar a rede ao acessar o site. Assim que o carregamento do site é concluído surge uma solicitação de download de um executável, alegando o propósito de atualizar o navegador, após o download e permissão de execução, o navegador redireciona a página para outro endereço URL *greatrecipesforme.com* que possui uma interface idêntica ao anterior, porém, com os produtos vendidos no site original sendo ofertados gratuitamente.  A análise do arquivo de log desta operação mostra que após uma conexão ter sido estabelecida entre o computador de origem e o site de destino *yummyrecipesforme.com*, já na camada de aplicação o browser solicita dados do site utilizando o método **HTTP : GET** através do protocolo **HTTP**, que inicia o download do arquivo malicioso, que em seguida à sua execução realiza o redirecionamento do usuário para o site clone.  Um analista sênior confirmou o comprometimento do site original, que ocorreu através de alteração em seu código fonte, com a adição de um código javascript que faz a solicitação do download malicioso ao visitante, e a análise do arquivo baixado encontrou o script que faz esse redirecionamento.  Posteriormente foi descoberto que a senha da conta do administrador ainda estava definida como a senha padrão e também não havia nenhum tipo de controle como autenticação de dois fatores, estes fatos juntamente com a alteração das credenciais da conta do administrador são fortes indícios de que o atacante possivelmente já tinha conhecimento do login e senha desta conta ou utilizou um ataque de força bruta para obter o acesso. |

|  |
| --- |
| **Sessão 3: Recomende uma remediação para ataques de força bruta** |
| Uma medida essencial de segurança que é recomendada, e que pode evitar que qualquer uma das hipóteses de comprometimento levantadas ocorra, é a autenticação de dois fatores, pois além das credenciais de login e senha, exige que quem está tentando obter o acesso à conta verifique sua autenticidade através de outro meio, como um dado biométrico ou uma senha de uso único enviada por email ou telefone.  Outras duas medidas recomendadas incluem, políticas mais rígidas na criação de senhas, ou seja, senhas que não incluam datas ou sequências obvias de letras ou números e também limitar a quantidade de tentativas de login. |