TAG 1 – Engenharia Social

Nome: Thalles Nonato Leal Santos

Ataque de engenharia social usando redes sociais

Objetivo: Conseguir dados pessoais de uma vítima que saiu para viajar através das redes sociais dela.

Situação: Uma família viaja para outro lugar, supondo que assim como a maioria das pessoas, os membros dessa família tem acesso a internet e postam sobre essas viagens em suas redes sociais (Facebook, Instagram, Twitter, etc...), as únicas informações que tenho são essas contas e através das postagens deles conseguirei obter uma forma de conseguir os dados pessoais dos membros dessa família. Para fins de dificultar a invasão, consideremos a família composta por apenas 3 pessoas (Pai, Mãe e Filho(a) adolescente).

Malwares e equipamentos utilizados: Trojan de acesso remoto, celular e redes sociais das vitimas.

Estratégia: Monitorar as redes sociais das 3 pessoas, dando enfoque as localizações. Focaremos principalmente no filho, por ser mais jovem, é o mais propício a fazer muitas postagens nas redes sociais, além disso tentarei me aproximar dele através de um perfil falso e com isso conseguir seu número e , seu whatsapp, farei isso tentando causar empatia com ele, para isso fingirei ter os mesmos gostos da vítima, tentando me aproximar como um amigo, e , dependendo do status civil do filho(a) e sexualidade, o fake pode até ser alguém com interesses amorosos, em determinado momento da conversa entrarei no assunto viagens, tendo em mente que ele falará que está de viagem próximo a região em que nosso fake “mora”, falarei que moro próximo e tenho parentes que trabalham com o ramo de hotéis e sempre oferecem promoções para turistas e que informaria a esse parente que estão de viagem, para ele ligar para família e apresentar um desconto na hospedagem. Após saber aonde estão e conseguirmos o número de uma das vítimas, pesquisaremos pontos turísticos nessa região e principalmente estabelecimentos que oferecem serviços que necessitam CPF (como hotéis, pousadas e em alguns casos restaurantes, para a nota fiscal), para dar a entender que conhecemos a região. Me passarei por um atendente que seria uma espécie de parente do nosso fake que trabalha em um hotel, escolheremos algum hotel perto de onde a família está, pegaremos informações sobre hotel e me passarei por um funcionário dele. Após isso, argumentarei que foi passado a informação através do nosso fake que a família está de viagem e temos uma promoção para atrair turistas para o nosso hotel, essa promoção consiste em cobrir o preço do hotel em que eles

já estão hospedados e ainda se propondo a fazer um serviço melhor, e , em caso de não ter atendido a satisfação do cliente, devolveremos o dinheiro, todavia para isso acontecer teríamos que conversar diretamente com o responsável financeiro da família (no caso, pai ou mãe desse filho(a)). Visto que ninguém gostaria de fazer seus pais pagarem mais caro, com uma promoção dessa, e incluindo o fato de ser alguém próximo ao nosso fake, criaria uma situação de confiança e muito provavelmente a vítima passaria o número de seu pai, ou de sua mãe. Com isso, já temos em nosso repertório: número de pelo menos duas vítimas e suas redes, todavia ainda não conseguimos dados importantes. Agora entraremos em contato com o responsável financeiro, nos passaremos pelo mesmo atendente de hotel, conversaremos com o responsável financeiro via telefone e após passarmos informações suficientes sobre o hotel para criar a confiança necessária para ele querer se hospedar conosco, falaremos que será necessário responder um formulário para sabermos em que precisamos melhorar em relação ao hotel em que estavam hospedados as vítimas, e para tornar nosso serviço ainda mais confiável para a vítima, pedimos um e-mail de contato ou até podemos mandar o formulário pelo whatsapp. Nesse formulário, será solicitado que seja preenchido individualmente por cada membro da família, além disso será feito um google formulário para tentar passar confiança para a vítima (atrelando a ideia do formulário a algum serviço da google que o hotel use, tentando dar uma ideia de “ligação” entre a google e o hotel), e nele conterá informações desejando saber o que o hotel anterior não ofereceu com qualidade e o que acha que poderemos fazer para aumentar o conforto deles durante a estádia ao nosso hotel, e como requisito para sabermos se os clientes realmente responderam o questionário e estão aptos para receberem a promoção, pedimos que eles nos mostrem ao chegar ao hotel o arquivo de confirmação que enviaremos, e nesse arquivo conterá um vírus trojan de acesso remoto (RAT) , que será executado pelas vítima. Com isso, poderemos acessar infinitas coisas, logs, contas de e-mail , dados pessoais que foram armazenados em compras pela web, conversas e nos maiores casos logs das vítima em contas de banco, terminando assim nosso ataque com excito, e conseguindo roubar os dados pessoais da família.