PROCESSO SELETIVO - Grupo de Resposta a Incidentes de Segurança

Nome: Fernanda Veiga Gomes da Fonseca
TAG - Engenharia Social - Entrega: 14/02/2020

Inicialmente, pensei em utilizar as técnicas do Google Hacking para encontrar cadastros de funcionários da empresa “Anônima Ltda.” em diferentes lojas e sites, pois algumas pessoas utilizam o e-mail da empresa nos mesmos. Entretanto, após algumas tentativas, não obtive o resultado desejado em minha busca.

Dessa forma, optei por descobrir o domínio de e-mail através de uma busca simples no Google e consegui obter inclusive os domínios de departamentos da empresa. Em seguida, levantei os nomes mais comuns no Brasil para ter uma lista de e-mails possivelmente utilizados na “Anônima Ltda.”.

Posteriormente, utilizei o endereço de correio eletrônico “seguranca@nonima.com.br” e elaborei um texto alertando sobre um ataque recente ao site da empresa, solicitando, pois, alteração das senhas dos funcionários. Foi empregado um tom de urgência na mensagem através do pedido para encaminhamento do e-mail a todos os colegas da empresa de forma que as medidas fossem tomadas rapidamente. Assim, foi possível que a mensagem chegasse a endereços verdadeiros de e-mail utilizados pelos funcionários.

No corpo do e-mail foi deixado um link para a utilização da técnica de “phishing”. Após clicar nele, a pessoa era redirecionada para uma página com layout semelhante aos sites legítimos da empresa. Comprei um certificado para o domínio de forma que o navegador não impedisse o acesso e um funcionário menos atento se tranquilizasse apenas em ver um site https.

Era solicitado o nome de usuário, a senha atual e uma nova senha. Após o preenchimento das informações, era exibida uma mensagem conforme a mudança de senha havia sido feita com sucesso. Após a obtenção do usuário e da senha “antiga”, consegui acesso ao ambiente restrito do site da empresa e pude encontrar informações sensíveis,

as quais poderiam ser vazadas caso a técnica tivesse sido utilizada por criminosos. Considerando que a maioria dos usuários não testa a nova senha cadastrada, houve tempo hábil para acessar o sistema. Em poucos casos, funcionários testaram a nova senha logo em seguida, porém foi possível acessar o sistema com o usuário e a senha verdadeiros antes.

De maneira a aprimorar o ataque, poderia ser usado um script para envios com um determinado intervalo de tempo para os e-mails não serem detectados como spam. Juntamente, para diminuir o trabalho humano, um gerador automático de endereços de e-mail pode ser utilizado para concatenar as combinações dos nomes com o domínio de e-mail.