Departamento de Segurança da Informação e Comunicações – **DSIC** - *dsic.planalto.gov.br/*
Centro de Tratamento de Incidentes de Redes do Governo – **CTIR Gov** - *www.ctir.gov.br/*

Recomendação nº 01/2019 – Golpe de *Phishing*

Data de Publicação: 17/01/2019

1. Descrição

Atacantes vêm concentrando esforços na exploração de vulnerabilidades dos usuários, uma vez que é mais complexo atacar ou fraudar com sucesso um servidor (ativo computacional) de uma instituição.

Esses atacantes, aqui tratados como golpistas ou fraudadores, se utilizam de técnicas de engenharia social e por diferentes meios e discursos, procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas.

Existe vasta gama de golpes na internet, esta Recomendação se dedicará a tratar da fraude definida como *Phishing*:

Phishing, *phishing scam* ou *phishing-scam*, é o tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

Esta fraude é comumente propagada por envio de e-mail, porém é cada vez mais frequente a sua disseminação via mensagem de texto (SMS) ou ainda por aplicativos de troca de mensagens (WhatsApp e outros).

2. Impacto

Este tipo de fraude pode ocasionar a suas vítimas:

- extravio e divulgação de informações sensíveis;
- destruição de informações;
- indisponibilidade de serviços computacionais comprometidos;
- furto de identidade;
- prejuízo financeiro;
- danos a imagem;

3. Dispositivos Afetados

Ainda que a utilização de ferramentas *antiphishings* ou antimalwares previna ou mitigue parte considerável desses golpes, alguns deles chegam às vítimas sem serem detectadas. Isso ocorre porque muitas vezes as mensagens maliciosas são enviadas de remetentes conhecidos (que podem ter sido invadidos ou forjados) ou ainda por se utilizarem quase que exclusivamente o ataque de engenharia social para persuadir as vítimas.

O ambiente computacional é meio para o ataque de engenharia social. Por esse motivo os mais diversos dispositivos podem ser afetados.

4. Recomendações

Prevenção

Uma das melhores formas de prevenir a ataques desse tipo é se utilizar de bom senso. O golpista tenta se utilizar das emoções da vitima, tentando atrair sua atenção: provocando curiosidade, oferecendo vantagem financeira, instigando urgência.

A "Cartilha de Segurança para Internet" do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) recomenda as seguintes ações para prevenir esse tipo de golpe:

- fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em links;
- questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
- fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
- não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada;
- seja cuidadoso ao acessar links. Procure digitar o endereço diretamente no navegador Web;
- verifique o link apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o link real para o *phishing*. Ao posicionar o mouse sobre o link, muitas vezes é possível ver o endereço real da página falsa ou código malicioso;
- utilize mecanismos de segurança, como programas *antimalware*, firewall pessoal e filtros *antiphishing*;
- verifique se a página utiliza conexão segura. Sites de comércio eletrônico ou Internet Banking confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados;
- verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador Web será diferente do endereço correspondente ao site verdadeiro;
- acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

Mitigação

Em caso de suspeita de recebimento de *phishing* ou comprometimento de credenciais, notifique imediatamente a equipe de tratamento de incidentes computacionais, setor de segurança ou suporte de tecnologia da informação da sua organização.

Se suspeitar que tenham sido fornecidas informações sensíveis (por exemplo, suas credenciais), execute procedimentos para troca das credenciais ou bloqueio temporário de conta. Caso as informações sensíveis afetem terceiros, informe-os para que estes possam realizar mitigações dos possíveis impactos decorrentes.

5. Referências

- Cartilha de Segurança - https://cartilha.cert.br
- Catálogo de Fraudes - https://catalogodefraudes.rnp.br
- Phishing - https://www.avast.com/pt-br/c-phishing
- Spear Phishing - https://www.kaspersky.com.br/resource-center/definitions/spear-phishing

Equipe do CTIR Gov – *ctir@ctir.gov.br*