Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 04/2014 – *Phishing Message/Spear Phishing*.

1. Descrição do Problema

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.

Spear Phishing traduz-se como um ataque de *phishing* altamente direcionado. O atacante estabelece seu alvo (empresa, departamento, setor, funcionário,...), realiza sondagem de informações básicas, e explora uma falha humana: a dificuldade de avaliar corretamente a sensibilidade de uma informação e a veracidade da mensagem.

O CTIR Gov vem alertar para ocorrência de ataques direcionados à órgãos e entidades da Administração Pública. Alguns órgãos da APF foram vítimas de mensagens recentes do tipo *Spear Phishing* e, por isso, faz-se necessário recomendar a realização de campanhas de conscientização e de aplicação de políticas de segurança eficientes nessa instituição para conter ou mitigar este tipo de ataque.

As mensagens tentam convencer o usuário a realizar tarefas inerentes às atividades da organização, direcionando-o para sítios fraudulentos (*Phishing Site*), onde, normalmente, precisam informar credenciais de algum sistema válido.

A seguir, exemplos de *Phishing Site* capturados em algumas campanhas recentes:

Nas situações acima, a mensagem de *phishing* solicita que as referidas páginas sejam acessadas e que o usuário digite sua conta e senha do sistema corporativo.

2. Possíveis Riscos

Com a captura de credenciais de usuário, o atacante pode obter acesso às informações da Instituição, tanto no correio eletrônico quanto em sistemas, e pode lograr êxito em ações de invasão na rede corporativa, realizando diversas atividades maliciosas, tais como a interceptação, destruição ou modificação de ativos de informação, o envolvimento e participação de máquinas da Instituição em ataques de Negação de Serviço (DoS/DDoS), com consequente dano à sua imagem e da Admistração Pública.

3. Sugestões para Mitigação do Problema

Os links apresentados nas mensagens de *phishing* apontavam para o domínio [j.mp|69.58.188.45] que redirecionavam para subdomínios em [url.ph|31.170.164.241], portanto sugerimos acompanhar qualquer fluxo de saída para esses destinos.

Analisar e aplicar possíveis filtros em mensagens que façam referência a sistemas corporativos, como também monitorar os pacotes de saída, buscando expressões que correspondam à submissão de credenciais de usuários, quando for possível.

Aplicar política de senha eficiente, prevendo uma chave forte, alteração periódica de senhas, evitando repetições e reutilização de senhas antigas, e outros controles que evitem a quebra da segurança.

Recomendamos a preparação e documentação de ações e contramedidas que venham a ser aplicadas de forma imediata, em casos de ataque à organização. Essa preparação não impede o sucesso da atividade maliciosa, no entanto minimiza consideravelmente os possíveis prejuízos.

Dicas direcionadas aos usuários:

- não utilize a mesma senha para diversas finalidades, por exemplo, para sistemas corporativos, conta bancária, e-mail corporativo, e-mail pessoal etc;
- altere suas senhas periodicamente;
- não cadastre o e-mail institucional em listas de discussão e sítios não ligados ao trabalho;
- não clique em links e não abra anexos recebidos de remetentes desconhecidos;
- não envie e nem repasse mensagens com conteúdo impróprio, ofensivo ou do tipo corrente;
- não envie dados sigilosos da instituição para seu e-mail particular; e
- jamais repasse sua senha a terceiros.

Referências:

- http://cartilha.cert.br/golpes/
- http://pt.wikipedia.org/wiki/Phishing

Brasília-DF, 12 de Junho de 2014

Atenciosamente,

Equipe do CTIR Gov