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 01/2017 – Sequestro de contas de gerenciamento de domínio cadastradas no Registro.br

1. Descrição do Problema

Ações maliciosas para obtenção de acesso às contas de gerenciamento de domínio e alteração da configuração dos servidores DNS, direcionando os usuários para páginas fraudulentas.

2. Ameaças

Foram confirmados vários casos de sucesso desse tipo de ataque contra órgãos de governo e grandes empresas, os quais tiveram como consequência a alteração dos Servidores DNS daqueles domínios, com o consequente direcionamento dos acessos para páginas fraudulentas. Essas páginas podem conter códigos maliciosos que podem comprometer a máquina do usuário e até mesmo a rede de computadores da organização, por meio de download de malwares, exploração de vulnerabilidades nos aplicativos instalados no computador e nos equipamentos da rede de computadores da organização, afetando a segurança e a imagem de toda a instituição.

3. Métodos de Ataques

Os atacantes podem se utilizar de mensagens fraudulentas (*Phishing Message*) para obter as credenciais de administração do domínio, conforme exemplo a seguir:

Segurança Registro Br

Prezado Cliente, Sou Hugo Pedroso Trabalho na Area de Manutenção da Registro.BR, e Notei que sua conta precisa de uma atualização na questão De endereço

Faça o Login no site: http://2XX.XX.XXX.XXX/registrobr/

Preencha os Campos, Caso Ao contrario Sua conta Será Suspensa Por Motivos De Segurança, e todos os dominios ficaram forá do Ar.

Duvidas, Responda o Email

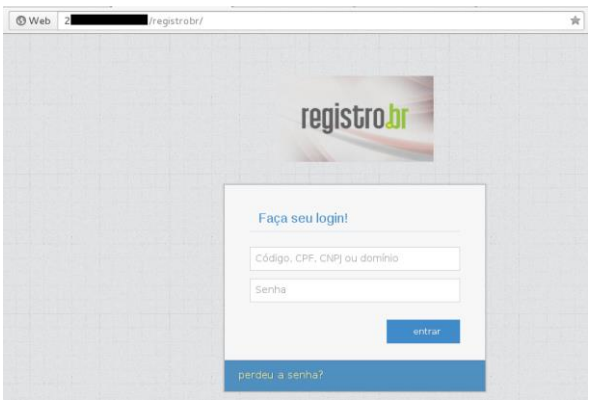

Figura 1 - Sítio Fraudulento hospedado no exterior que explora a imagem do Registro.br

Há também diversos relatos de comprometimento da conta de correio eletrônico do administrador, cadastrada como conta de recuperação de senha no sistema de registro. De posse dessa conta, o atacante solicita a recuperação da senha, através das opções do tipo "*Esqueci minha senha*", e consegue acesso ao Sistema de Registro.

4. Sugestões para Mitigação Problema

O Registro.br dispõe, desde março de 2013, da opção de autenticação por duplo fator, ou seja, um segundo controle de acesso aos recursos administrados por cada ID no Registro.br, conhecido também como "Verificação em Duas Etapas". Tal opção gera o recurso de *Token* do Registro.br e permite aos usuários aumentar a segurança de suas contas utilizando, além de suas senhas, um código de segurança.

O recurso de *Token* é o resultado do uso de uma aplicação que implementa autenticação em dois passos, do armazenamento de uma chave secreta num dispositivo portátil que é usado para geração de sequências numéricas variando a cada 30s (também denominado "código temporal") e da geração de um conjunto pré-informado de sequências numéricas que só se pode utilizar uma vez ("códigos de uso único").

A utilização do *Token* pode ser feita através dos aplicativos: *Google Authenticator* (Android ou iOS) ou *Authenticator* (Windows Phone). Estes aplicativos serão os responsáveis pela geração dos códigos temporários requeridos na autenticação.

Os códigos de uso único deverão ser usados sempre que não tiver acesso ao seu dispositivo móvel. O Registro.br recomenda que esses códigos sejam impressos e/ou guardados de maneira segura.

No entanto, ressaltamos que o serviço *Token* do Registro.br é optativo, sendo necessário ativá-lo seguindo as etapas descritas no sítio do Registro.br.

Deste modo, recomendamos firmemente que todos os admistradores de domínios dos órgãos e Entidades da Administração Pública, adotem a autenticação por duplo fator para gerenciar suas contas junto ao Registro.br. Lembramos que o uso de senha forte continua sendo necessário.

Recomendamos ainda, a leitura do Fascículo especial da Cartilha de Segurança para Internet, confeccionado pela equipe do CERT.br, dedicado ao recurso de proteção no acesso a uma conta, conforme referências abaixo.

Por fim, reforçamos que incidentes de segurança que envolvam a gestão de domínios da Administração Pública Federal devem ser comunicados imediatamente ao Registro.br pelo endereço hostmaster@registro.br, com cópias para cert@cert.br e para ctir@ctir.gov.br e exclusivamente para os casos de comprometimento de contas no sistema do registro, contactar o Registro.br (NOC 7x24) pelo telefone 11-5509-3510.

5. Referências:

- http://cartilha.cert.br/fasciculos/verificacao-duas-etapas/fasciculo-verificacao-duas-etapas.pdf
- https://registro.br/suporte/token.html

Brasília-DF, 10 de Janeiro de 2017.

Equipe do CTIR Gov