Alerta de Segurança 003/2012 - CGTI/VPGDI

Em 25 de junho de 2012

Prezados Gestores,

Estamos retransmitindo o Alerta de Segurança do Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov) encaminhando à Fiocruz.

1. Assunto

Comprometimento de sítios de órgãos e entidades da Administração Pública Federal (APF), Estados e Municípios, por meio de publicação de conteúdos incompatíveis, com spam de links/conteúdos (*spamdexing*).

2. Objetivo

a) Sintetizar o tipo de ataque;
b) Orientar as Equipes de TI da Fiocruz sobre formas de mitigação.

3. Problema

Os órgãos da Administração Pública vêm sofrendo sucessivos ataques de *spamdexing* em seus sítios, com motivação aparentemente comercial para a obtenção de vantagens econômico-financeira.

Nos últimos meses esses órgãos tem sido alvo constante desses ataques, que denigrem a imagem institucional e, em um contexto mais amplo, comprometem os domínios da APF, Estados e Municípios (“gov.br”, “jus.br”, “leg.br”, “mil.br”, dentre outros).

4. Apreciação/Análise

a) *Spamdexing* é a técnica de injetar, de forma deliberada e maliciosa, spams de links e de conteúdos em sítios web. O objetivo do invasor é aumentar a relevância de sítios maliciosos ou de fins comerciais em motores de buscas e dessa forma melhor ranqueá-los nas consultas ao *Google, Bing, Yahoo Search* e outros.
b) Essa forma de ataque explora as mesmas vulnerabilidades utilizadas para desfigurações de sítios, porém injetam códigos ocultos que referenciam sites de venda de produtos de vários

segmentos comerciais, como farmacêuticos, eróticos, marcas famosas ou com intuitos maliciosos.

c) Técnicas de dissimulação do ataque dificultam sua percepção por parte do usuário. Pode-se verificar o comprometimento do sítio por meio dos passos:
   i. Acessar a URL possivelmente comprometida;
   ii. Selecionar a opção "Exibir Código-Fonte" do navegador;
   iii. Procurar por termos como: VIAGRA - CIALIS - CHEAP - PRICE - COUPONS - DRUGS - DISCOUNT - BUY - PHARMACY - PURCHASE, etc.

d) A análise do código-fonte das páginas no navegador, em alguns casos, pode não ser suficiente para identificar a injeção de links ou conteúdos. Nesses casos é necessária a pesquisa por arquivos comprometidos, ou alterados, diretamente na console do servidor que hospeda os serviços web, na base de dados ou no campo de pesquisa do site. Caso se utilize alguma ferramenta para indexação do site, esta pode ser utilizada para pesquisa pelos termos indicados.

e) Em algumas situações, o código utilizado para injeção de conteúdo checa se o IP de origem da conexão pertence aos mecanismos de busca mais populares da Internet e utiliza técnicas de ocultação. Nesse caso, a injeção de código ocorre somente para os mecanismos de pesquisa e motores de busca, o que corrobora a informação de que a pesquisa no código-fonte do navegador pode não ser suficiente para a verificação da injeção de links ou conteúdos maliciosos.

f) Observa-se que, em alguns casos, a técnica de injeção dos links / conteúdos se dá por meio de cláusulas "*include*" no código-fonte. Nesses casos, a pesquisa pelos termos indicados não será efetiva, uma vez que referenciam outros domínios possivelmente comprometidos, sendo necessária então a análise dos códigos pesquisando por cláusulas como *include(), require(), request()* e outras.

g) Observa-se também o abuso de fóruns, livros de visita, comentários de notícias e de imagens com a injeção de conteúdos incompatíveis, através de spam de links/conteúdos. O abuso, na maioria dos casos, é facilitado pela deficiência no controle de acesso, na moderação dos fóruns ou controle de publicações nos sítios.

h) Os atacantes se valem de robôs automatizados que verificam essas deficiências e injetam os códigos desejados. Essa vulnerabilidade permite também os ataques *de SQL Injection, Cross Site Script* e outros.

5. Mitigação

a) Os ataques de *spamdexing* exploram vulnerabilidades já conhecidas e utilizam-se das mesmas técnicas empregadas para desfiguração de sítios. Assim, é fundamental a aplicação de patches de correção e atualização de softwares e gerenciadores de conteúdo, além de seguir as boas práticas de programação e "*hardening*" de servidores e serviços web, a fim de dificultar esse tipo de ataque ou coibir as suas tentativas.

b) Essas técnicas podem ser encontradas na Internet, em sítios comprovadamente confiáveis. Destacam-se duas publicações que resumem muito bem algumas medidas que devem ser adotadas:

- Práticas de Segurança para Administradores de Redes Internet, do CERT.br (http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf);
- Melhores Práticas de Codificação Segura OWASP - Guia de Referência Rápida (https://owasp.org/images/6/6f/OWASP_SCP_Quick_Reference_PT-BR_v1.2.pdf).

c) Tendo em vista a constatação de muitos sítios comprometidos pertencentes à Adminitração Pública Federal, Estados e Municípios, sugerimos a verificação dos servidores web e sítios diponibilizados na Internet, seguindo as etapas relacionadas no item Apreciação/Análise deste documento, implementando as medidas corretivas necessárias.

d) Percebe-se, ainda, o aumento no número de abusos de fóruns, com a injeção de links e conteúdos incompatíveis. Isso decorre da deficiência no controle de acesso, na moderação dos fóruns e no controle de autorização de publicações. O mesmo acontece na publicação de livros de visitas, comentários de notícias e de imagens. Sob o aspecto da segurança, é desaconselhável a disponibilização de qualquer conteúdo em sítios de órgãos e entidades da APF, Estados e Municípios sem a rigorosa avaliação e controle das informações que serão publicadas.

e) Além disso, percebe-se que as falhas de programação são o principal vetor de ataque a sítios da Internet. As falhas de segurança podem ser introduzidas em qualquer fase do ciclo de desenvolvimento de software. A seguir serão apresentados alguns procedimentos importantes relacionados à prática de codificação segura, extraídos do guia de referência do OWASP.

- Efetuar toda a validação dos dados em um sistema confiável, centralizando todo controle no servidor;

- Validar todos os dados provenientes dos clientes antes do processamento, incluindo todos os parâmetros, campos de formulário, conteúdos das URLs e cabeçalhos HTTP. Certificar-se também de incluir automaticamente mecanismos de checagem nos trechos de código JavaScript, Flash ou qualquer outro código incorporado;
- Validar dados provenientes de redirecionamentos. Os atacantes podem incluir código malicioso no conteúdo originário do mecanismo de redirecionamento, podendo contornar a lógica da aplicação e qualquer validação executada antes do redirecionamento;
- Validar tipos de dados esperados, intervalo de dados e o comprimento dos dados;
- Validar, sempre que possível, todos os dados de entradas por meio de um método que utiliza lista de caracteres ou expressão regular que define os caracteres permitidos;
- Se qualquer caractere potencialmente perigoso precisa ser permitido na entrada de dados da aplicação, certifique-se que foram implementados controles adicionais, como codificação dos dados de saída, APIs específicas que fornecem tarefas seguras e trilhas de auditoria no uso dos dados pela aplicação. Exemplos de caracteres "potencialmente perigosos": <, >, ", ', %, (,), &, +, \, \', \";
- Realizar o tratamento (sanitização), baseado em contexto, de todos os dados provenientes de fontes não confiáveis usados para construir consultas SQL, XML, e LDAP;
- Garantir os controles de autorização em todas as requisições, inclusive em scripts do lado do servidor, "*includes*" e requisições provenientes de tecnologias do lado cliente, como AJAX, Flash, etc;
- Restringir o acesso aos arquivos e outros recursos, incluindo aqueles que estão fora do controle direto da aplicação, somente a usuários autorizados;
- Criar Política de Controle de Acesso para documentar as regras de negócio da aplicação, tipos de dados e critérios ou processos de autorização de acesso para que os acessos possam ser devidamente concedidos e controlados;
- Implementar Política de Privilégio Mínimo, restringindo aos usuários apenas as funcionalidades, dados e informações do sistema que são necessárias para executar suas tarefas;

- Filtrar os parâmetros que contenham informações sensíveis, provenientes do HTTP referer, quando realizar apontamentos para sites externos;
- Restringir os privilégios do servidor web, dos processos e das contas de serviços para o mínimo possível de usuários;
- Prevenir a divulgação da estrutura de diretórios impedindo que robôs de busca façam indexação de arquivos sensíveis;
- Utilizar códigos PHP em modo seguro (*safe mode on*); dentre outras.

6. Conclusão

a) No caso da detecção de sítios comprometidos com *spamdexing*, o restabelecimento do servidor ao estado anterior ao ataque ou a simples exclusão dos arquivos comprometidos não são medidas suficientes para solucionar o problema. Sugerimos que sejam avaliadas e resolvidas as vulnerabilidades exploradas pelo atacante, além de verificar se o servidor possui outros comprometimentos.

b) Observamos que sítios comprometidos com a injeção de spam de links/conteúdos têm sido categorizados pelos mecanismos de busca (*Google, Bing, Yahoo Search* e outros) como "sítios potencialmente perigosos".

c) O presente alerta não tem a pretensão de esgotar todas as possibilidades que envolvem o assunto.

d) As informações constantes deste documento são baseadas nos dados coletados pelos mecanismos de detecção do CTIR Gov ou capitaneadas pelas análises dos incidentes.

e) O fornecimento dos detalhes dos incidentes ocorridos nas unidades da Fiocruz à CGTI auxilia na avaliação de tendências e divulgação de alertas mais rotineiros e cada vez mais técnicos.

f) Toda notificação de incidente à CGTI deve ser feita exclusivamente para o endereço abuse@fiocruz.br;

g) Recomenda-se que as informações aqui contidas restrinjam-se exclusivamente à área de TI da Unidade;

h) Saiba mais sobre o Spamdexing (textos em inglês) em:

- http://www.webspam.org/seo-spam-what-is-spamdexing
- http://en.wikipedia.org/wiki/Spamdexing

Contatos:

Serviço de Segurança da Informação – (21) 3885-1768 – seguranca@fiocruz.br

Equipe de Tratamento e Resposta a Incidentes em Redes - (21) 3836-2127 – etir@fiocruz.br

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações