



OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

04/2023

Abuso de Sítio Eletrônico de Governo - SPAMDEXING

Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

Abuso de Sítio Eletrônico de Governo - SPAMDEXING

Conforme estatística do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov, o **spamdexing** é o segundo abuso de *site* de maior ocorrência no Governo Federal. Para compreender o **spamdexing**, vamos expor a ação de otimização dos mecanismos de busca na *internet*, ou *Search Engine Optimization* (SEO).

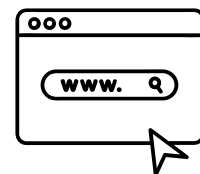


O SEO é o mecanismo que verifica o conteúdo de um *site* para executar a classificação e ordenação deste a partir dos termos relevantes inseridos pelos usuários, quando pesquisam algo na *internet*. O SEO é baseado nas palavras-chave usadas no conteúdo do *site* e nos *links* de entrada vindos de outros locais da *web* (*backlinks*) para este *site*.



Quando se trata de otimizar um *site* pelo SEO, o *link building* é uma das medidas mais importantes para obter uma boa posição em mecanismos de pesquisa populares. A presença de *links* de *spam* dificultará a visibilidade de um *site* e interromperá sua classificação pelo SEO.

Spamdexing ou SEO *Spam* é técnica de ataque que tem por objetivo a manipulação deliberada de índices de mecanismos de pesquisa, de maneira inconsistente, com o objetivo de burlar o sistema de indexação, de forma a alterar a relevância ou proeminência dos recursos indexados.



O **spamdexing** tornou-se um método altamente lucrativo usado por *hackers* para alterar as classificações SEO de um *site* e redirecionar usuários legítimos para *sites* de *spam* ou, até mesmo, de *phishing*.

Outra razão para esse tipo de ataque é que, ao redirecionar os usuários para *sites* maliciosos, os *hackers* podem roubar dados, obter acesso a informações de cartão de crédito por meio de compras ilegítimas, senhas de acesso a conteúdo, etc.



Técnicas de ataque mais comuns e soluções

Assim como o *defacement*, o **spamdexing** é um ataque oportunista. Os *hackers*, nesse caso, não atacam *sites* específicos. Eles realizam varreduras (*scans*) buscando vulnerabilidades em diversos *sites* simultaneamente e atacam aqueles que estiverem vulneráveis. Entre as vulnerabilidades mais exploradas estão:

1

versões desatualizadas dos aplicativos utilizados no *site*;

2

plug-ins e temas vulneráveis; e

3

senhas de acesso fracas.

Listamos abaixo as técnicas mais comuns utilizadas pelos *hackers* para executar um ataque de *spamdexing*.



1) Inserção de *links* de *spam* em páginas existentes em um *site*.



2) Injeção de páginas com *links* e conteúdo com *spam*. Geralmente, essas páginas são projetadas para manipular mecanismos de pesquisa ou fazer tentativas de *phishing*.



3) Injeção de código malicioso nas páginas do *site*, geralmente *JavaScript* malicioso diretamente no *site* ou em *iframes*, causando o redirecionamento de páginas do *site* atacado para outros *sites*. O redirecionamento não autorizado mostra conteúdo diferente aos usuários e mecanismos de pesquisa ou mostra aos usuários conteúdo inesperado que não atende às necessidades originais. Exemplos comuns de redirecionamentos não autorizados:

- a. mostrar aos mecanismos de pesquisa um tipo de conteúdo e redirecionar os usuários para algo diferente; e
- b. exibir páginas normais para usuários de computadores e redirecionar usuários de dispositivos móveis para um ambiente de *spam* diferente.



4) Uso de textos e *links* ocultos, adicionando conteúdo em uma página apenas para manipular os mecanismos de pesquisa sem que seja visível para visitantes humanos. Os principais exemplos disso são:

- a. uso de texto com fonte branca em fundo branco;
- b. ocultação de texto com uso de uma imagem;
- c. uso do mecanismo *Cascading Style Sheets* (CSS) para posicionar o texto fora da tela;
- d. definição do tamanho ou da opacidade da fonte como "0" (zero); e
- e. ocultação de um *link* vinculando apenas um pequeno caractere, por exemplo, um hífen no meio de um parágrafo.

O *Spamdexing* geralmente leva a uma perda de *ranking* do *site* infectado, uma vez que a entidade responsável pelo mecanismo de busca geralmente aplica penalidades a *sites* com má qualidade de construção de *links*. As penalidades podem ocorrer de duas formas:

- manualmente: nesse caso, a equipe de *spam* da instituição, que gerencia o mecanismo de pesquisa, revisa o perfil e aplica uma penalidade. Essa revisão pode ser desencadeada por uma reclamação de *spam* de um concorrente, por denúncias de usuários ou pelo acionamento de uma pesquisa algorítmica pela presença de *links* de *spam* no *site*. Nesse caso, é possível que o *webmaster* do *site* contaminado receba uma mensagem informando que foi detectado o uso de técnicas que violam regras de uso;
- por algoritmo: sistemas de verificação de qualidade que automaticamente aplicam a penalidade. Um *site* que receba uma penalidade algorítmica não será notificado – como ocorre na penalidade aplicada manualmente – mas testemunhará imediatamente uma queda do tráfego de acesso.

A fim de determinar se um *site* está infectado com **spamdexing**, é importante realizar as seguintes atividades, no mínimo:



utilizar ferramentas de análise em busca de picos suspeitos no tráfego ou na classificação de palavras-chave;



verificar o *status* do *site* no ambiente da ferramenta de busca. Apesar de não ser capaz de informar efetivamente sobre o **spamdexing**, ela informará sobre a existência de conteúdo prejudicial, como a existência de *backlinks* estranhos, o que é um bom indicativo de que o *site* provavelmente é vítima de *spamdexing*;



utilizar ferramentas disponíveis nos mecanismos de busca mais populares para verificar o *status* de indexação, *queries* de pesquisa, erros de rastreamento e otimizar a visibilidade do *site*. De uma forma geral, essas ferramentas notificam automaticamente por *e-mail* se o *site* estiver comprometido; e



utilizar *scanners* de *spam* avançados disponíveis.

É importante ressaltar que existem soluções de segurança, que, além de auxiliar na atividade de detecção de **spamdexing**, também auxiliam na remoção do **spamdexing** e reparação do *site*.

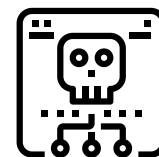
Caso o abuso tenha sido detectado, deve-se iniciar imediatamente a limpeza do *site*. Cada momento que o *site* permanece infectado com **spamdexing** corre-se o risco de sofrer sérias penalidades, além do prejuízo a imagem da organização responsável por aquele ambiente *on-line*. Em especial, o *site* pode ser colocado na lista de banimento pelos mecanismos de pesquisa para não aparecer nos resultados da pesquisa.



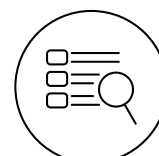
É possível excluir manualmente os códigos de **spamdexing**, mas essa é uma tarefa complexa e demorada pois:

- os códigos maliciosos geralmente estão ocultos em diversos pontos do *site* infectado. De qualquer maneira, deve-se tomar especial cuidado na verificação do cabeçalho e do rodapé do *site*, pois esses são os locais mais utilizados nos ataques por injeção de código malicioso; e
- geralmente o processo de limpeza requer conhecimento e experiência em codificação. Algumas das técnicas utilizadas implicam em aplicar comandos SQL para remover os *posts* com *spam*, os comentários com *spam* e limpar as meta-tabelas do *site*.




A fim de garantir a completa limpeza de **spamdexing** é recomendável a utilização de uma solução de segurança confiável, que possa analisar o *website*, detectar os códigos maliciosos e excluí-los, além de identificar possíveis *hacks*.



Após a finalização do trabalho de limpeza do *site* e correção das vulnerabilidades exploradas pelo autor do **spamdexing**, será necessário reenviá-lo para indexação. Caso o *site* tenha sinalizado por conteúdo hackeado, será necessário enviar o *site* para revisão da instituição responsável pelo mecanismo de busca.



Boas práticas para evitar ser vítima de spamdexing

- ✓ aplicar atualizações de segurança constantemente. Recomenda-se manter os *plug-ins* e outros aplicativos do *site* atualizados com as correções (*patches*) de segurança mais recentes. Ignorar atualizações pode deixar todo o *site* aberto para uma infecção de *spam* de SEO;
- ✓ obrigar o uso de senhas fortes, principalmente para proteger o acesso a áreas sensíveis do *site*; 
- ✓ monitorar regularmente do *site*. Essa atividade ajuda os administradores a descobrir e entender os problemas de segurança nos *sites*. Muitas vezes, não se percebe que o *site* foi vítima de **spamdexing** até que ocorra uma penalização por violação das regras de uso dos mecanismos de busca, o que também leva à perda de credibilidade nos mecanismos de pesquisa;
- ✓ usar um *firewall*. Um *firewall* de aplicativo da web (WAF) é uma solução essencial para evitar uma infecção de **spamdexing**. O WAF inspeciona e filtra o tráfego entre cada aplicativo da *web* e a *internet*. O WAF também alivia a carga administrativa ao garantir testes de segurança de aplicativos da *web* adequados de maneira contínua. Ao ajudar a definir diretrizes e regras de forma proativa, as equipes de segurança de aplicativos podem monitorar o que deve e o que não deve ser permitido por meio de um WAF. No entanto, apesar do WAF ser capaz de proteger um *site* contra várias ameaças desconhecidas, como ele não foi projetado para evitar todos os tipos de ataques, ele funciona melhor como parte de um conjunto de ferramentas que ofereça suporte a um programa de segurança de aplicativo abrangente; 


O Departamento de Segurança da Informação e Cibernética (DSIC) recomenda, ainda, que:

- sempre haja o *backup* do *site* anterior a infecção. Sem um *backup* funcional do *site*, o processo de recuperação será muito mais complexo; e
- qualquer usuário que constate um incidente cibernético, como o **spamdexing**, informe imediatamente a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da instituição.

O DSIC solicita ainda que propostas de temas, sugestões ou outras contribuições sejam encaminhadas ao e-mail educa.si@presidencia.gov.br para fomentar futuras publicações da OSIC. Por fim, outros conceitos podem ser verificados no glossário do DSIC disponível em:

<https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1>

TLP: CLEAR

<https://www.gov.br/gsi/pt-br/ssic> <https://www.gov.br/ctir>

Sugestões: educa.si@presidencia.gov.br