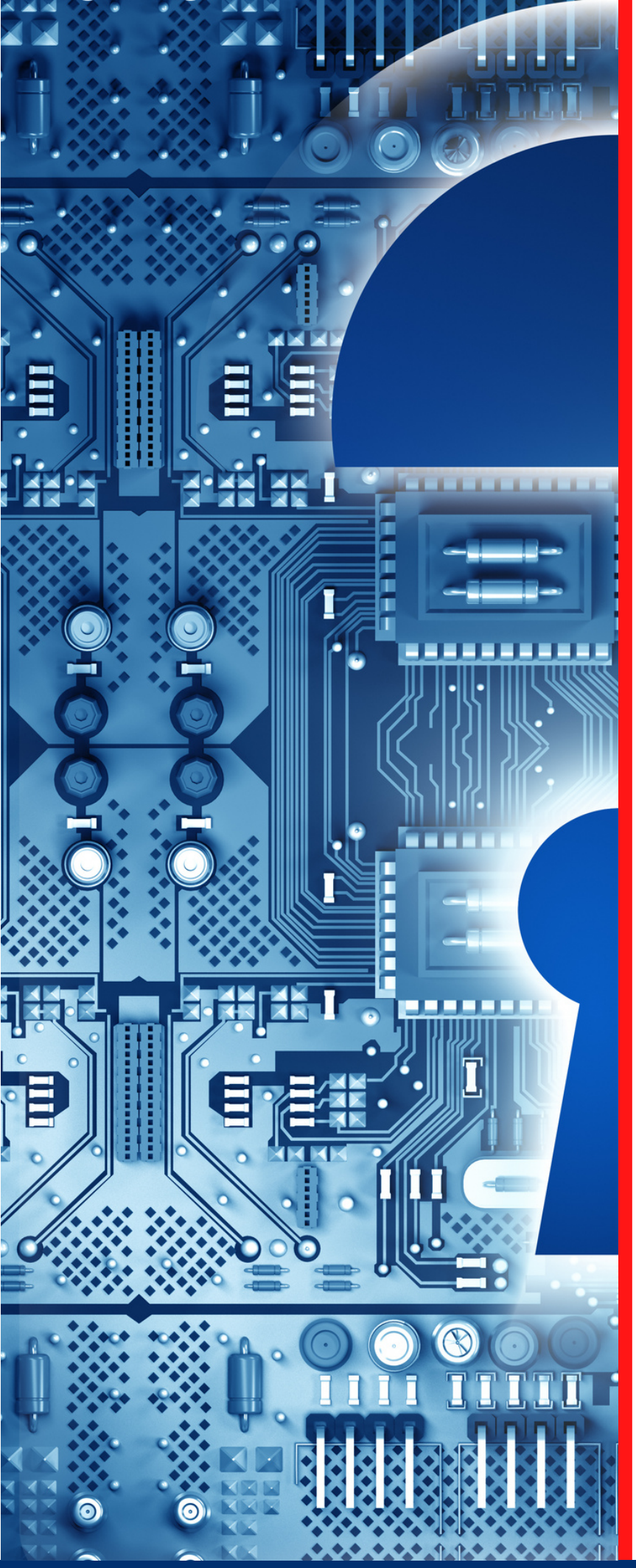


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

03/2023

Abuso de Sítio Eletrônico de Governo - *DEFACEMENT*

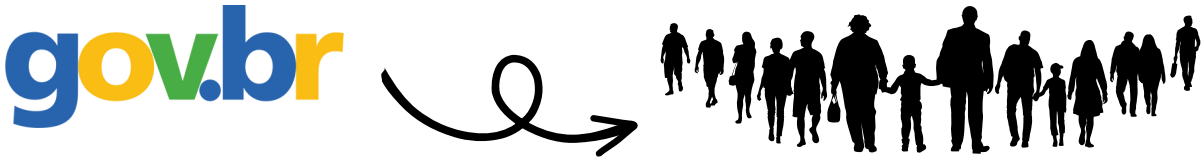
Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

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

TLP:CLEAR

Abuso de Sítio Eletrônico de Governo - *DEFACEMENT*

Os sítios institucionais na *internet* ou, em inglês, *sites*, são importantes meios de comunicação entre governo e sociedade. Por meio deles, são disponibilizados serviços essenciais ao cidadão e informações úteis para toda a sociedade.

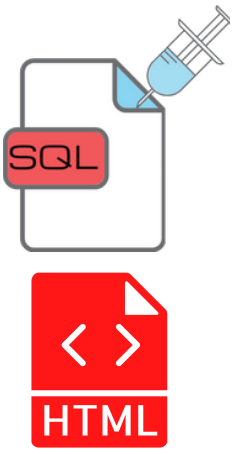


Devido à importância e à consequente visibilidade, acabam sendo alvos de atividades maliciosas como ataques às suas páginas e abusos de seus serviços, que podem afetar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Conforme estatística do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov, o abuso de site de maior ocorrência no Governo Federal é o ataque de desfiguração de *site*, mais conhecido como ***defacement***. Ele pode ser definido como um ataque cibernético que visa atingir uma página da *web* específica, explorando suas vulnerabilidades.

Muitos consideram esse ataque pouco importante, pois entendem equivocadamente que se limitaria a um invasor que altera o conteúdo legítimo de páginas do *site* para um texto ou uma imagem de protesto que represente ideias ou pensamentos sobre um determinado assunto.

Entretanto, é importante entender que ***defacement*** se refere a um ataque em que tanto a aparência, como o conteúdo de um *site* ou página da *web* é afetado, modificando, alterando e até excluindo o conteúdo originalmente disponibilizado, atacando sua disponibilidade e sua integridade.



Isso significa, portanto, que o próprio código de construção da página afetada (HTML) está sendo alterado sem permissão. Porém, vale destacar que o ***defacement*** não se concentra apenas no código HTML, podendo atingir também outros componentes da página *web*. Uma das técnicas de exploração de vulnerabilidades utilizadas no ***defacement*** é o ataque de injeção de SQL, em que um código malicioso é executado usando a linguagem HTML[1], os endereços das páginas na rede (URLs) e outros campos onde os dados podem ser manipulados.

Isso pode permitir ao invasor o acesso a dados reservados armazenados no *site* ou a modificação de dados armazenados nos bancos de dados, através de operações de inserção, atualização e/ou exclusão de dados, acessados por meio da página.

Causas mais comuns

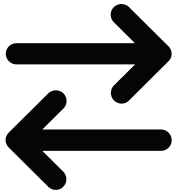
As causas mais comuns de ***defacement*** são contramedidas de segurança insuficientes, falta de atualizações periódicas do sistema e medidas defensivas deficientes. Vale destacar que servidores configurados incorretamente representam vulnerabilidades que podem ser facilmente detectadas por ferramentas de sondagem empregadas por *hackers*. Uma vez detectada uma vulnerabilidade, um ataque pode ser iniciado imediatamente, pois a maioria dos ataques de ***defacement*** são oportunistas.

Com o avanço da digitalização, o número de sites vitimados por ataques de ***defacement*** aumentou ao longo dos anos, tornando o tema muito importante. As técnicas do atacante variam, assim como as vítimas.

Os tipos mais comuns de ataque:

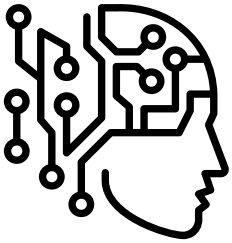
1. *bugs* de aplicativos da *web* (27,22%);
2. injeções de SQL (18,00%);
3. envenenamento de URL (3,76%);
4. invasão de servidor de transferência de arquivos FTP[2] (3,11%);
5. engenharia social (3%);
6. configuração incorreta de compartilhamento (2,38%);
7. invasão de servidor SSH[3] para acesso remoto (2,18%);
8. invasão de servidor de e-*mail* (1,15%).

As técnicas de detecção de defacement podem ser agrupadas em três categorias:



- **detecção baseada em anomalias** - As técnicas tradicionais baseadas em anomalias envolvem a comparação de *checksum*[4] e ferramentas de comparação *DIFF*, que comparam a página em exibição no momento com uma referência *off-line*, sendo que a mais simples e rápida para páginas *web* estáticas é a primeira.

- **detecção baseada em assinaturas -** A técnica baseada em detecção de assinaturas envolve padrões de ataque conhecidos (regras) que são armazenados para monitorar a página da *web*. Se houver uma correspondência com as regras armazenadas, haverá um alarme para um ataque. No entanto, esse tipo de técnica é eficiente apenas para tipos de ataques conhecidos, sendo incapaz de identificar novos tipos de ataques.



- **técnicas de aprendizado de máquina -** Técnicas avançadas como o aprendizado de máquina têm desempenhado um papel vital na classificação de páginas da *web* em desfiguradas ou normais, sendo que diferentes métodos têm sido propostos. No entanto, um fator importante é que a precisão da detecção deve ser de alto nível e os alarmes falsos (falsos positivos) devem ser reduzidos para menos de 1% em função das elevadas exigências de recursos de computacionais para lidar com grandes conjuntos de dados envolvidos.

Boas práticas recomendadas

Com o avanço da digitalização, o número de *sites* vitimados por ataques de ***defacement*** aumentou ao longo dos anos, tornando o tema muito importante. As técnicas do atacante variam, assim como as vítimas.

Para evitar ataques de ***defacement***, recomenda-se adotar, dentre outras, as boas práticas abaixo.

1. Controlar os *uploads* para o site: se um *site* permite *uploads* de arquivos, alguém pode fazer *upload* de um arquivo malicioso e sobrescrever um dos arquivos existentes. Caso seja necessário permitir o *upload* de arquivos, é conveniente adotar as seguintes regras de compartilhamento de arquivos:
    - alterar a permissão dos arquivos recebidos para que o servidor não tente executá-los;
    - armazenar os arquivos recebidos fora do diretório raiz;
    - modificar os nomes dos arquivos ao armazená-los para que um *hacker* não possa acessá-los em momento futuro;
    - limitar os tipos de extensões de arquivo permitidos e seu tamanho; e
    - verificar com um *antimalware* cada arquivo recebido.
2. Adotar o princípio do menor privilégio: consiste em dar acesso às pessoas dentro da organização apenas ao que é absolutamente necessário para o desempenho de suas responsabilidades, e nada mais além disso.
3. Utilizar protocolo HTTPS no *site* em substituição ao HTTP: com isso, um certificado SSL[5] protege a transferência de informações confidenciais entre o usuário e o servidor, bem como dificulta que invasores criem uma versão falsa do *site*, além de ajudar a ganhar a confiança do usuário.
4. Proteger as informações de *login*: a proteção das informações de *login* é a primeira barreira contra uma invasão. Para isso, deve-se sempre adotar boas práticas como:
    - utilizar sempre senhas fortes;
    - obrigar a troca periódica de senhas;
    - não utilizar e bloquear as contas padrão do tipo ADMIN, USER, GUEST;
    - limitar o número de tentativas de *login*; e
    - usar autenticação de dois fatores (2FA) ou multifator (MFA).
5. Realizar o *backup* regularmente.
6. Realizar auditorias de vulnerabilidade constantemente.
7. Usar o teste *CAPTCHA*[6] para proteger contra tentativas de acesso por meio de *bots*.
8. Utilizar *plugins* apenas quando necessários.
9. Manter o *software* do servidor *web* atualizado.

O Departamento de Segurança da Informação e Cibernética (DSIC) recomenda que qualquer usuário que constate um incidente cibernético, como o *defacement*, 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

Informações complementares

1. **Linguagem HTML:** HTML (*Hypertext Markup Language*) é uma linguagem de marcação utilizada para criar páginas da *web*. Ele define a estrutura e o conteúdo de uma página da *web*, incluindo textos, imagens, *links* e outros elementos.

2. **Arquivos FTP:** FTP (*File Transfer Protocol)*, é um protocolo de transferência de arquivos utilizado para transferir arquivos entre um computador cliente e um servidor na *internet* ou em uma rede privada. É amplamente utilizado para *upload* ou *download* de arquivos em *websites* e servidores.

3. **Servidor SSH:** servidor SSH (*Secure Shell)*, é um servidor que oferece conexões seguras (via protocolo SSH) para acesso remoto e gerenciamento de sistemas, como servidores e sistemas UNIX/Linux.

4. ***Checksum*:** *checksum* é uma verificação de integridade de dados que compara um valor numérico gerado a partir de um arquivo de dados com uma cópia do mesmo arquivo. Se as *checksums* forem iguais, significa que o arquivo não foi corrompido ou alterado durante a transferência ou armazenamento.

5. **Certificado SSL*:*** um certificado SSL (*Secure Socket Layer*) é um tipo de certificado digital que fornece segurança ao estabelecer uma conexão segura entre um *site* e um navegador. Ele criptografa as informações trocadas entre o *site* e o usuário, garantindo que dados confidenciais, como informações de *login* ou informações de cartão de crédito, não possam ser interceptados ou acessados por terceiros.

6. ***CAPTCHA:*** CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*), é uma ferramenta de segurança que determina se um usuário é humano ou não. Eles aparecem como uma série de caracteres distorcidos ou imagens que precisam ser digitados ou selecionados para provar que o usuário é humano.