Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Defacement

Edição nº22
Abril/2022

O "defacement" ou "deface" é um tipo de ataque hacker que consiste no processo de modificação do conteúdo que é exibido em um site. Geralmente, o invasor não costuma acessar a base de dados nem derrubar o servidor ou sequestrar as máquinas responsáveis: ele simplesmente deixa uma mensagem para os usuários e responsáveis, colocando o recado por cima da estrutura original.

O deface é comparado com o ato de pichar um muro ou parede, com a diferença de que a parede é a página de outra pessoa. Por conta disso, os defacers também são chamados de pichadores. A maioria desses ataques tem cunho político, objetivando disseminar uma mensagem do autor do ataque para os frequentadores do site alvo.

Esses ataques podem também ter cunho pessoal, transformando-se em uma espécie de troféu para o autor, como se fosse um prêmio pela sua capacidade de penetrar na segurança de determinado sistema. No Brasil, sites do governo, de políticos ou de partidos, acabam se tornando alvos de defacement.

Para ter acesso a sites, o invasor precisa ganhar acesso a um ambiente que normalmente não é autorizado. Ele pode conseguir esse acesso utilizando métodos de engenharia social, phishing ou buscando por brechas ou vulnerabilidades no servidor web, erros na aplicação web ou mesmo em aplicações da hospedagem onde o site se encontra. Após identificar a brecha, o atacante faz a inserção de um código malicioso que pode resultar na alteração da página principal ou parte dela.

Dentre os prejuizos causados por este tipo de ataque, podemos citar:

- Depreciação do aspecto visual do site;
- Impactar na perda de visitantes do site a curto e a longo prazos, isso porque o conteúdo fica indisponível até a situação ser resolvida;
- Perda da confiança do usuário devido à sensação de insegurança no site, por ele não ter como ele saber se além do deface, há algum outro tipo de comprometimento de segurança na página;
- Existe um problema relacionado aos mecanismos de busca, como o Google, por exemplo, pois eles costumam não listar sites comprometidos nas páginas de resultados de pesquisa.

Algumas soluções para evitar ou corrigir o defacement:

- O primeiro passo é retornar a página original que foi alterada durante o ataque. Para isso, é importante ter sempre um backup recente do sistema;
- Manter todos os plugins e softwares terceirizados atualizados para a versão mais recente;
- Utilizar a ferramenta website application firewall ativada em seu site para reduzir o risco de infecções no site;
- É importante que todas a brechas sejam encontradas e corrigidas;
- Atualizar as senhas de acesso periodicamente, utilizando senhas fortes;
- Ter uma política de segurança adequada, assim como padrões de codificação seguros;
- Monitorar qualquer tráfego suspeito.

Como já foi dito antes, esses ataques se aproveitam de vulnerabilidades que podem ser exploradas para ações mais graves. Por isso, antes de subir a página original do seu site, não esqueça de corrigir as vulnerabilidades para mitigar ataques futuros.

Fique ligado: no próximo mês, falaremos sobre
Cuidados necessários na internet utilizando as máquinas de trabalho!

Tribunal Regional Eleitoral - RN