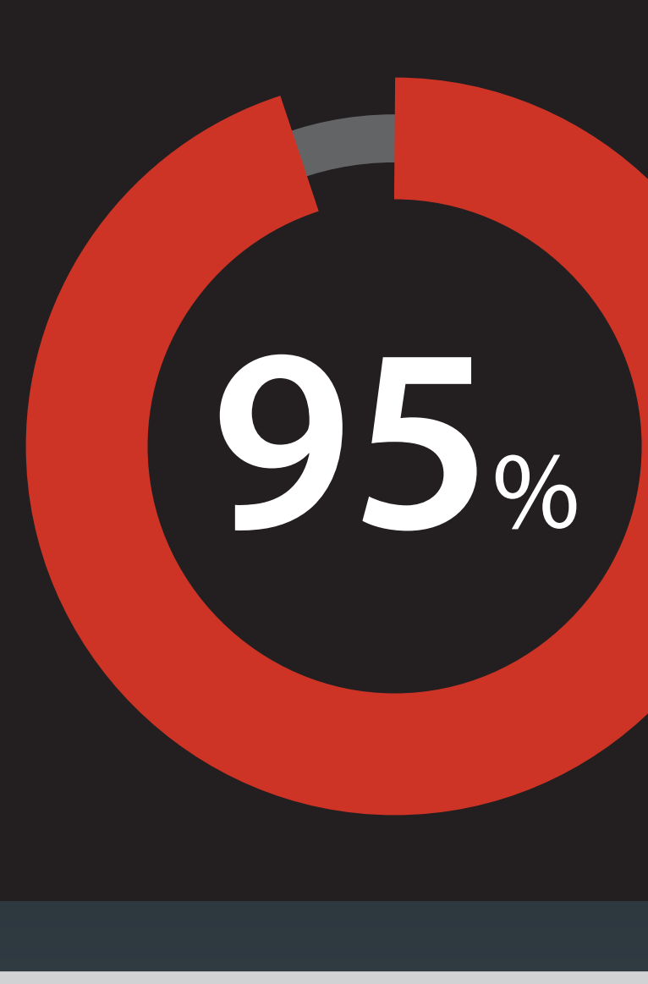
Seu site está protegido?

Os criminosos tentarão de tudo para explorar seu site e usar as informações dos seus clientes. Nenhum dono de site deve estressar-se com os problemas após uma intrusão, **desde a intercepção de processos de pagamento à perda de lealdade dos seus clientes.**



do tráfego orgânico se perde quando um site é notificado e entra em uma lista negra, o que impacta rapidamente as **vendas** e as **receitas** do site.

A maioria dos hacks de sites ocorre devido à exploração de código inseguro. O vetor de ataque está escondido dentro das muitas linhas de código que compõem seu site. Quando uma falha de segurança se torna conhecida, todos os sites vulneráveis podem ser comprometidos em um período de tempo muito curto.

AS 3 PRINCIPAIS VULNERABILIDADES DE SOFTWARE

Ataques de Dia Zero

Vulnerabilidade de software que ainda não foi divulgada ao público, o que significa que não possui nenhuma correção disponível para proteger o site.

CMS, Plugins, & Temas Desatualizados

Seu site é composto de temas, plugins, arquivos de núcleo e arquivos personalizados em seu servidor. Se uma correção é lançada, mas você não pode atualizar, então seu site se torna um alvo fácil.

Common Vulnerabilities & Exposures (CVE)

Risco de segurança envolvendo uma falha no código em execução no seu site usado por um invasor com o objetivo de obter acesso não autorizado.

A escolha do serviço de segurança para o seu site começa com o **reconhecimento da sua necessidade.**

O **melhor tipo de segurança é feito em camadas,** combinando ferramentas e processos para dar cobertura aos três elementos da segurança de sites.

3 ELEMENTOS DA SEGURANÇA DE SITES

Proteção

Sistema de segurança do site que monitora e controla o tráfego do seu site através de uma rede de servidores intermediadora desse processo.

Detecção

O processo de escaneio e monitoramento do código fonte e do banco de dados de um site em busca de malware e falhas de segurança.

Resposta

Um sistema ou serviço de segurança de sites que remove todo tipo de malware, backdoor, phishing, malvertising, ou qualquer infecção do seu site.

CUIDADO COM ESTES TIPOS DE ATAQUES

O processo automático de adivinhar as senhas dos sites até que se encontre uma combinação.

Os atacantes deixam muitas maneiras de entrar em um site hackeado, para que continuem a usá-lo mesmo após a vulnerabilidade ser corrigida.

Um ataque que muda a aparência de um site, geralmente ao incluir imagens e mensagens na página principal do site.

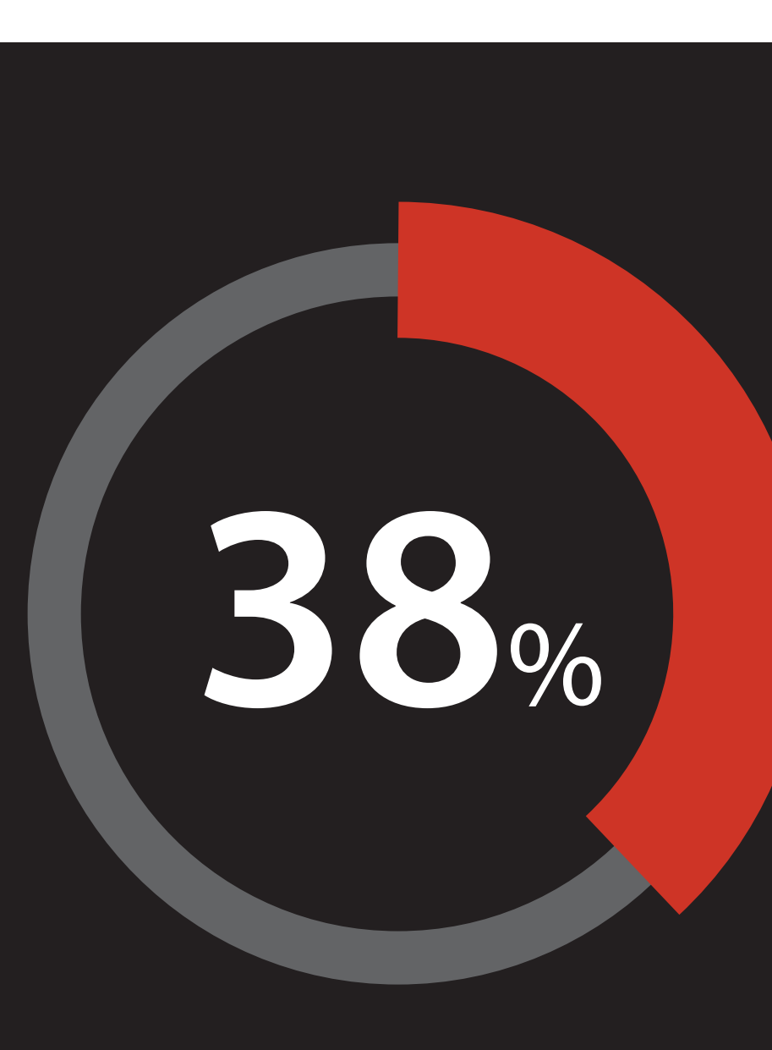
Um ataque que tira um site do ar com tráfego falso enviado de muitos computadores comprometidos.

Um site hackeado espalha a infecção para outros sites que compartilham a mesma conta de servidor.

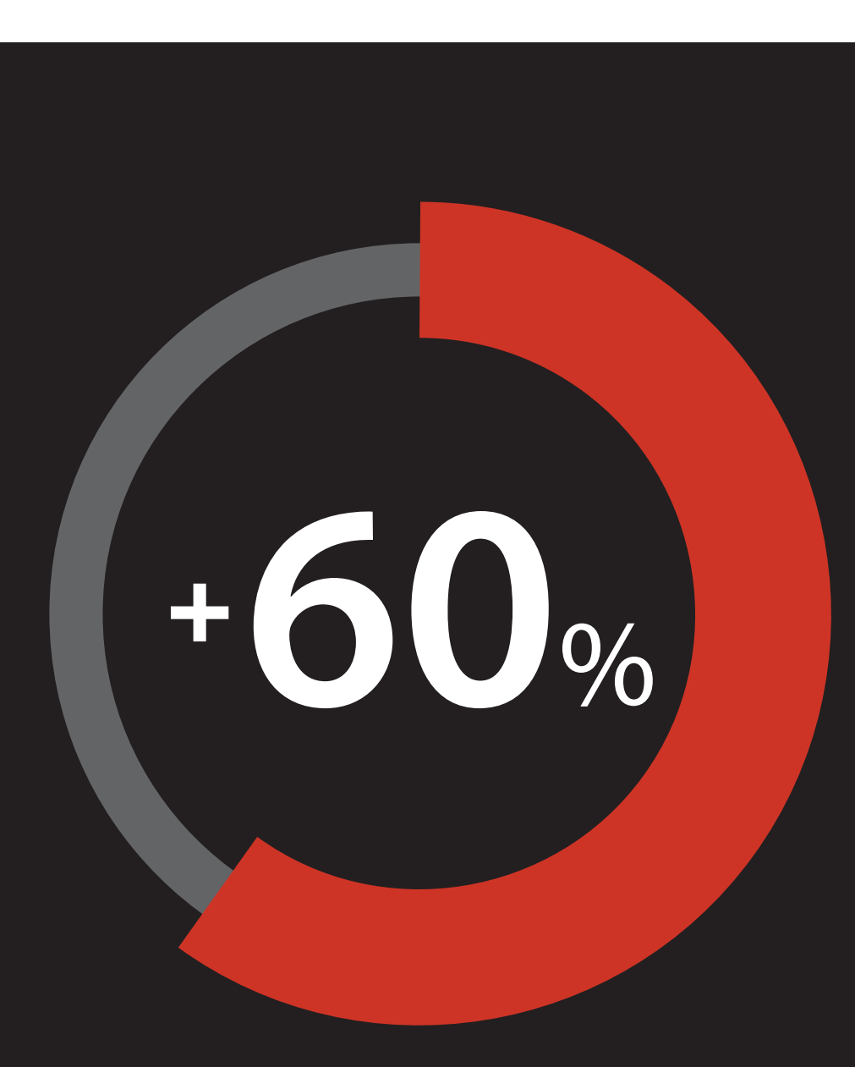
Um ataque que infecta sites com palavras-chave de spam e links para tentar enganar os motores de busca, com o objetivo de melhorar a classificação de conteúdos maliciosos.

Quando o ambiente do host é configurado usando práticas ruins, software de servidor vulnerável e outras falhas.

Ataque usado para infectar sites com anúncios maliciosos por meio de uma rede vulnerável de anúncios.



Search Engine Poisoning (SEP) é o ataque que mais cresce, segundo a base de clientes da Sucuri.



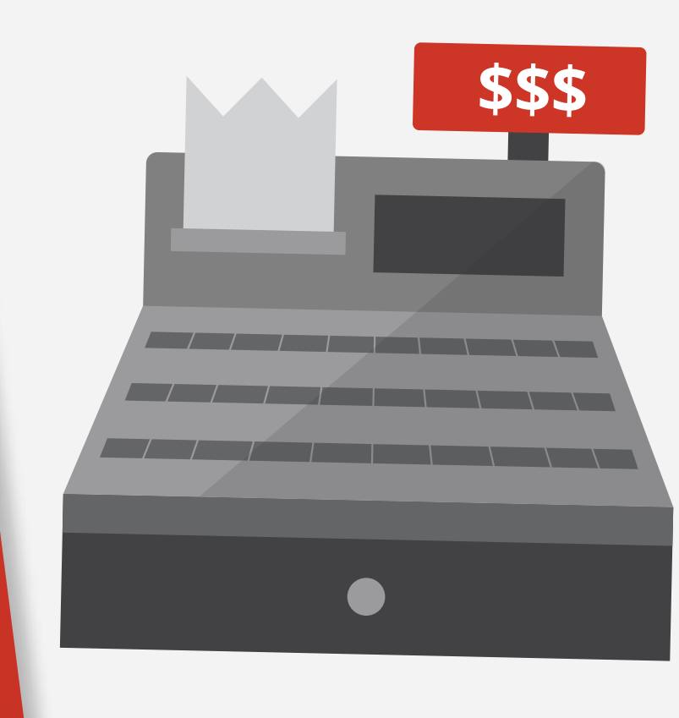
de sites infectados tem algum tipo de **Backdoor** no seu sistema, segundo a base de clientes da Sucuri.

CONHEÇA SEU INIMIGO

Ataques de hackers afetam todos os tipos de sites.
É importante entender como um hacker pode te atacar.

Páginas de Checkout em Sites Ecommerce

Alvo:
Sites Ecommerce



Conhecidos por:

- Enganar os usuários infectando a página de checkout para redirecionar os usuários a sites maliciosos.
- Desenvolvido para roubar as informações dos cartões de crédito dos compradores.
- Perda de consumidores, receita e possíveis multas de órgãos regulatórios.

Contaminação Cruzada de Sites em Servidores Compartilhados

Conhecidos por:

- Uma vez que os hackers ganharem acesso a um site no servidor, podem infectar outros sites que compartilham as mesmas permissões do servidor.

Alvo:
Sites Servidores Compartilhados

Tráfego Redirecionado para Site Malicioso

Alvo:
Servidor DNS

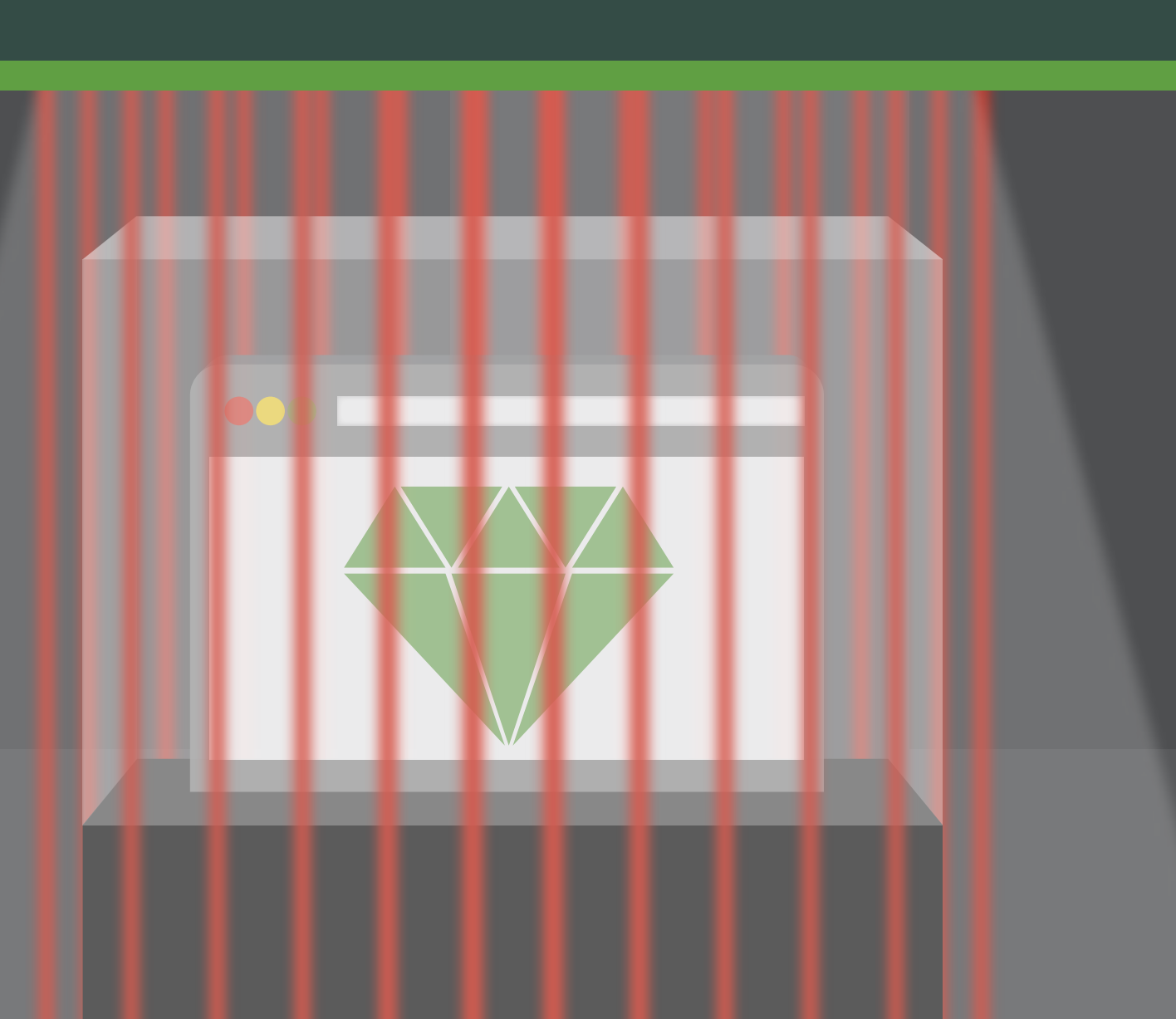
Conhecidos por:

- O ataque adiciona um servidor de nome para os DNS Records de um site.
- Muito difícil de identificar o hack, porque não está no site em si.

Você tem um plano?

Os criminosos tentarão explorar seu site e tomar vantagem da informação sensível do servidor

Você precisa de reflexos apurados e defesa robusta para impedir que os hackers infectem seu site. Ao remover os métodos que os hackers usam para penetrar o seu código inseguro, as tentativas do autor do malware tornam-se inúteis. **Elimine todas as vulnerabilidades de segurança do seu site e as substitua por uma página de bloqueio para qualquer um que tente explorar seu site.**



DEFESA EM PROFUNDIDADE

Implemente controles de defesa complementares sobrepostos (defesas em camadas) desenvolvidos para identificar e mitigar ataques.

Você não pode garantir que seu site é impenetrável. Sem as devidas camadas de defesa, seu site pode sofrer de um pedaço de código vulnerável. São várias as preocupações: plugins, SSL, Apache... Não se trata somente de responder às alertas e às atualizações. Falhas ainda não descobertas e pontos fracos permitem que malfeitores entreguem malware e spam, afetando seus visitantes e a sua reputação.

Sucuri
Real People. Real Security.

Para obter mais informações sobre os nossos serviços e para entender como a Sucuri pode responder às necessidades de segurança de sites da sua empresa, entre em contato conosco no **info@sucuri.net** ou no telefone **1-888-873-0817**. Visite nosso site no **sucuri.net/pt**