Sites Invadidos

O que fazer para se proteger e resolver uma eventual invasão em seu site Wordpress.

Índice interativo:

Tipo de Invasões: Como e Por que as Invasões (normalmente) ocorrem

Atualmente mais de 40% de todos os sites na web são feitos pelo Wordpress, sendo um dos CMSs mais utilizados nos dias de hoje. Toda essa visibilidade é um dos fatores que chamam a atenção dos atacantes, além é claro, do código do Wordpress ser aberto, facilitando a análise por busca de vulnerabilidades.

Além, dos motivos apresentados acima temos mais algumas razões que normalmente fazem com que sites sejam invadidos:

- **CMS (Wordpress), plugins ou temas vulneráveis**
  Os atacantes frequentemente aproveitam-se de vulnerabilidade descobertas no Wordpress ou em aplicações de terceiros (plugins e temas) para comprometer um site. Normalmente esses ataques são automatizados e direcionados a essas vulnerabilidades. Por isso é tão importante manter seu WordPress e demais plugins e temas sempre atualizados.

- **Senhas fracas**
  Um tipo de ataque bastante conhecido é o ataque de *brutal force (força bruta)* que visa adivinhar, dentre milhares de combinações, as credenciais de acesso para seu site. Se você estiver usando credenciais padrões (Ex: usuário padrão **admin**), senhas fáceis de adivinhar (Ex: **admin123**) e não utiliza nenhum plugin de segurança, ataques de força bruta são usados para conseguir facilmente o acesso completo ao seu site para o atacante.
- **Permissões de arquivo incorretas**
  Seu provedor de hospedagem utiliza várias regras para controlar o acesso aos arquivos de seu site, como permissões de acessos aos arquivos e pastas. No entanto, caso essas permissões estiverem equivocadas pode ser uma brecha bastante preocupante que os hackers podem se aproveitar e facilmente explorar.

Sinais de que seu site WordPress foi hackeado

Existem diversos sinais que podem indicar que seu site foi comprometido, confira abaixo os sintomas mais comuns para notar:

- **Você não consegue "fazer o login" em seu Painel de Administração de seu Site:**
  Algumas vezes ao ter seu site atacado os hackers ou removem os usuários do banco de dados de seu site ou ainda alteram a senha dos usuários administradores impedindo o acesso a seu site. Caso note que isso ocorreu você pode tentar redefinir sua senha clicando na opção de "Esqueci a senha" caso o hacker não tenha excluído seu usuário do banco de dados.

- **Seu plugin de segurança e monitoramento notificou uma alteração inesperada nos arquivos de seu site:**
  Caso você não tenha acessado ou mesmo alterado algum arquivo de seu site é bem suspeito você perceber que houve alteração em arquivos de seu site. Salvo quando ocorre atualizações automáticas do próprio Wordpress, se você encontrou alterações nos arquivos principais do seu site ou então seu plugin de segurança o notificou que houve alterações inesperadas em algum(s) arquivo(s) isso pode ser um indício de que seu site possa ter sido comprometido e que há um invasor que possa estar utilizando a estrutura de seu site para envio de spam, criar backdoors[1] em seu site ou ainda executar algum código malicioso.
  Além disso, qualquer arquivo novo com nome suspeito ou ainda com código suspeito deve ser tratado com extrema cautela e urgência na análise do site.

- **Seu site foi envolvido em alguma atividade incomum ou ainda houve uma denúncia contra seu site nos levando a desativar - mesmo que temporariamente - seu site:**
  Algumas vezes, através de alguma auditoria interna notamos algum comportamento incomum de um site, com isso iremos bloquear temporariamente seu site e você irá receber uma mensagem avisando sobre a suspensão de seu site. O mesmo ocorrerá, por exemplo, caso seu site se envolva, por estar invadido, em algum incidente de ataque a outros sites ou mesmo com algum ato ilícito.

- **Ao acessar seu site o navegador ou o antivírus seu ou de seu visitante acusará de site inseguro:**
  Caso o navegador Google Chrome ou outro navegador exibir uma mensagem de aviso ao visualizar o site, é provável que seu site tenha sido hackeado. Em casos assim o site acusado entra em uma lista negra (*blacklist*) de autoridade do Google (Google Safe Browsing).

- **O Google Search Console exibe uma mensagem de aviso informando que seu site foi invadido ou está hospedando algum malware:**

---

[1] **Backdoor** é um método, geralmente secreto, de entrada/acesso irrestrito em um determinado sistema ou site. Como o próprio nome sugere é uma porta de acesso não documentada que permite ao atacante/administrador entrar em um sistema de forma facilitada.

Sites cadastrados no Google Search Console conseguem enviar ao proprietário do site em que está vinculado quando um site estiver comprometido. As informações repassadas pelo Google podem ser bastante valiosas para ajudar a identificar conteúdo de spam ou códigos maliciosos presente em seu site.

- **Seus clientes estão reclamando de clonagem de seus cartões ou cobrança indevida:**
  O roubo de informações de cartões de crédito é algo extremamente preocupante porém bastante comum em ataques como esse o que pode gerar muitas dores de cabeça para o dono do site, isso porque as informações de cartões de créditos de seus clientes adquiridos através de um site invadido pode ser facilmente vendidos e trocados por dinheiro no mercado negro ou usados para fazer compras fraudulentas. Em sua grande maioria os ataques a sites de comércio eletrônico se dão por alguma vulnerabilidade conhecida em alguns plugins, temas e outros componentes de terceiros, por isso é tão importante manter todos os elementos de seu site atualizado, instalar apenas componentes de fontes confiáveis e não utilizar plugins ou temas craqueados (*nulled*).

- **Javascript estranhos no código do site:**
  Os hackers normalmente utilizam algumas técnicas de ofuscação (esconder ou embaralhar o código para este se tornar confuso ou ilegível), formatação e comentários de código para ocultar o malware da visualização. Ainda um pequeno trecho de código JavaScript malicioso pode ser usado para coletar detalhes ou senhas de cartões de créditos ou outras informações de um site invadido.

- **Lentidão em seu site:**
  Na maioria dos casos de invasão a sites os malwares usam muitos recursos do servidor onde o site está hospedado tornando o site invadido lento e levarem muito mais tempo para serem carregados para seus visitantes.

- **Seu site está redirecionando para outro local:**
  Muitos invasores injetam redirecionamentos maliciosos para enviar o tráfego de seu site para alguma página fraudulenta de spam ou algum anúncio estranho (normalmente onde aparece um robôzinho). Os invasores fazem isso para aumentar o tráfego e SEO de suas páginas ou páginas associadas a ele. Então se você ou o visitante de seu site foi redirecionado para alguma página de destino de spam seu site provavelmente foi invadido.

- **Seu site realiza alterações ou modificações sem que ninguém tenha realizado tais alterações:**
  Por exemplo, se a página foi modificada ou substituída por uma nova página, foi adicionado alguma página ou elementos em uma página já existente isso é um forte indício que seu site foi invadido.

- **Páginas com escritas japonesas (Kanjis) indexadas ao Google:**
  Quando você realiza uma busca de páginas de seu site que estão indexadas ao Google (pesquisa= **site:seusite.com.br**) caso apareça algumas páginas com escritas estranhas como na imagem abaixo é um forte indício que seu site está invadido.

Fora os sinais apresentados acima existem vários outros que também pode ser um forte indício que seu site foi invadido, tais como:

- Tela branca da morte (ao acessar seu site);
- Seus usuários recebem a tela vermelha do Google informando que seu site não é seguro;
- Redirecionamentos para sites aleatórios (e maliciosos) ao acessar seu site ou clicar em algum link ou botão;
- Páginas desconfiguradas;
- Usuários suspeitos criados em seu site. Às vezes seu site permite que pessoas se cadastrem para receber alguma newsletter ou ainda ter acesso a um painel do usuário. No entanto algumas vezes esses usuários se aproveitam de alguma vulnerabilidade de seu site e conseguem acesso para realizar uma série de ações maliciosas em seu site.
- etc

Esses são alguns dos sinais mais comuns que indicam que seu site em Wordpress foi hackeado.

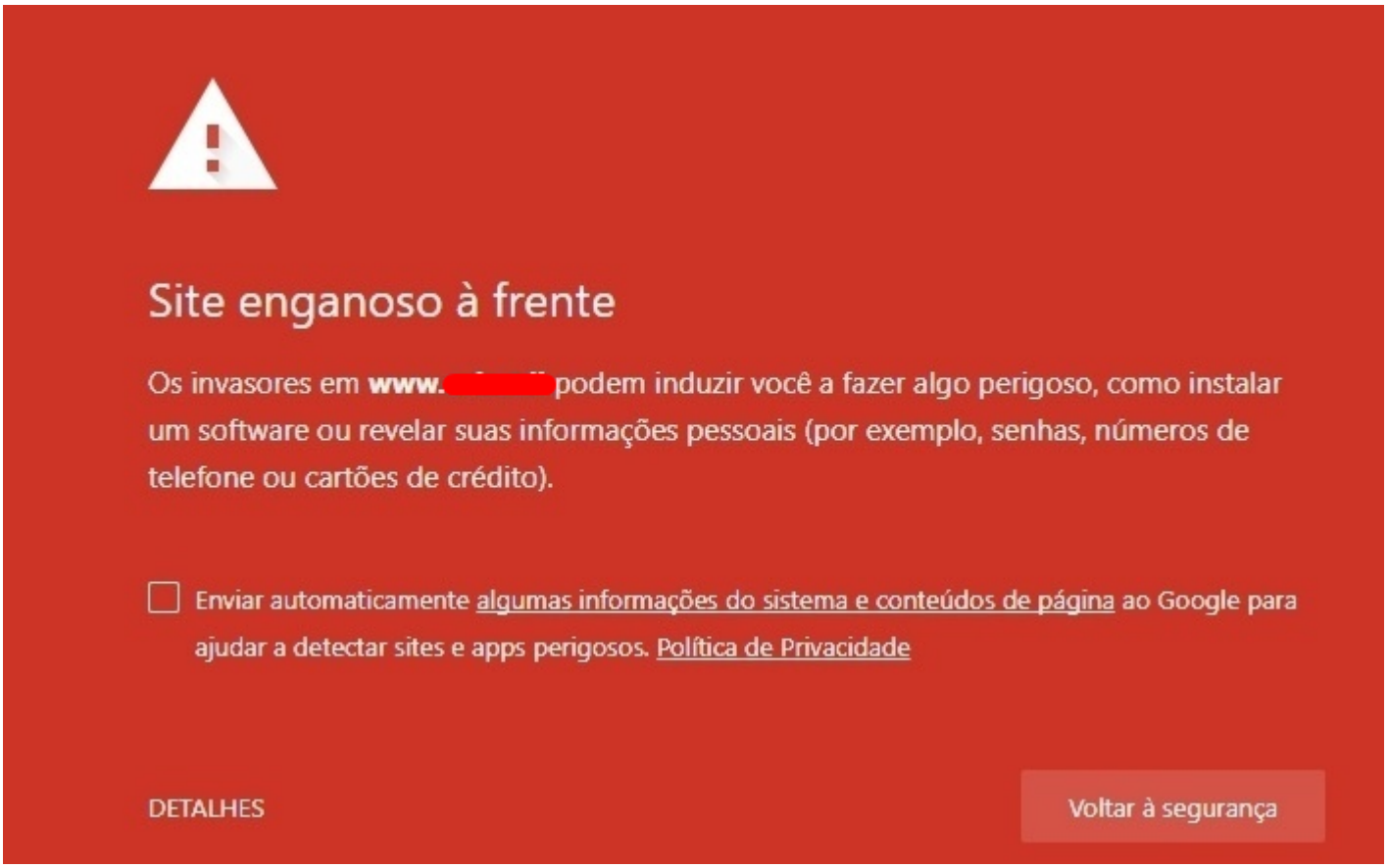
É completamente possível realizar a limpeza e recuperação de um site WordPress hackeado, mesmo sendo um processo mais moroso e minucioso onde exige do analista um certo nível de conhecimento técnico de hospedagem de sites e programação.

Mesmo depois de analisar nossos passos a passos perceba que você não consegue realizar os procedimentos para a limpeza de seu site recomendamos a contratação de um especialista em remoção de vírus ou a utilização de ferramentas de remoção de vírus que poderão lhe auxiliar nesta questão.

Cuidados: O que fazer após seu site ser hackeado?

Uma vez identificado que seu site foi hackeado é importante tomar alguns cuidados para não piorar a situação do seu site. Para isso é de extrema importância você realizar a limpeza com seu site **pausado**, isso porque caso você não o faça as chances são você comece o processo de limpeza e a invasão reconhecendo a exclusão de alguns arquivos façam sua cópia em vários outros locais mais escondidos, o que será praticamente impossível de você remover por completo toda incidência de vírus de seu site.

Além disso, outro ponto que deve-se levar em consideração nesse processo é que durante a execução de seu site hackeado você pode piorar a situação de seu site e domínio entrando em algumas blacklist mundiais bem como o do google que pode gerar então a temida tela vermelha do Google.



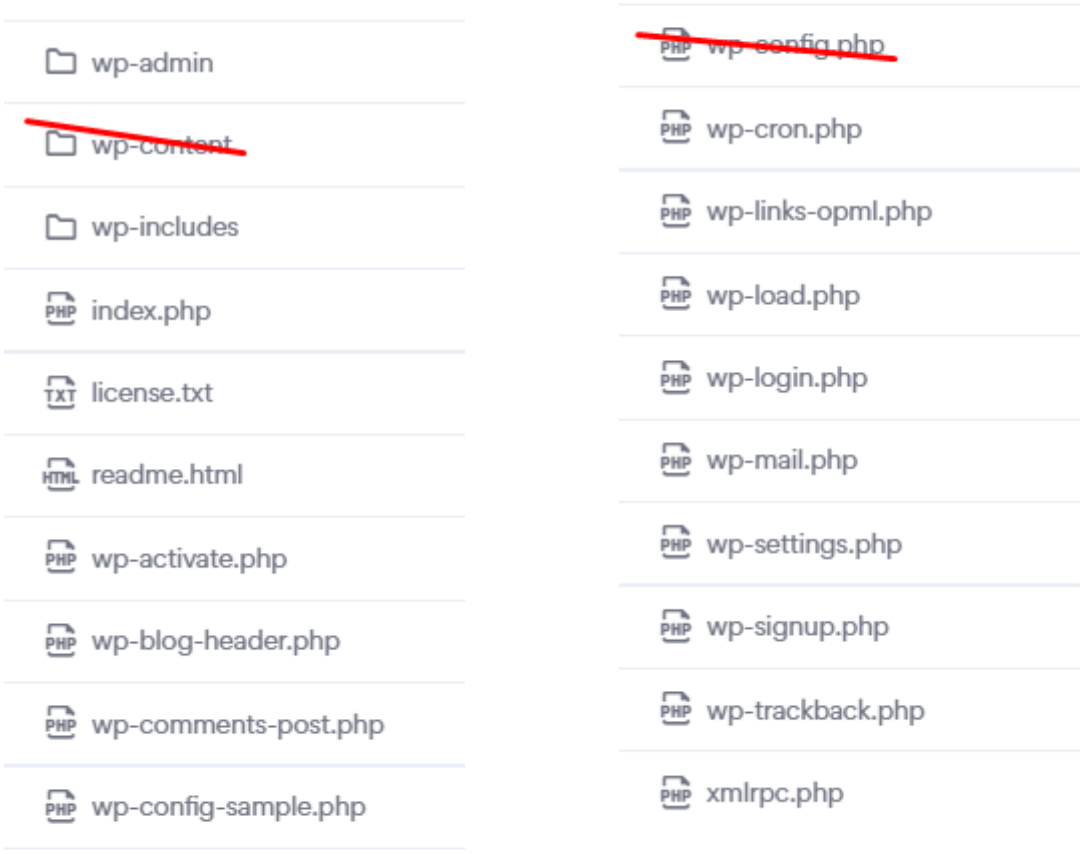
Então o melhor a se fazer após verificado que seu site está infectado/hackeado é realizar o download de todos os arquivos (e banco de dados) que estão atualmente em sua hospedagem para um ambiente para análise. Esse ambiente pode ser outra hospedagem ou mesmo o seu computador para que você consiga analisar toda a estrutura do site além de conseguir fazer uma verificação mais minuciosa dos arquivos do site.

Uma vez que você passe por uma situação de invasão de seu site é extremamente importante, a princípio trocar todas as senhas de acesso:

- Senhas de FTP e SSH;
- Senhas de acesso e seu site;

Como limpar seu site?

Existem várias etapas a serem seguidas se o seu site Wordpress foi invadido. Independentemente de como o seu site WordPress foi comprometido, abaixo vou repassar algumas considerações e medidas que você poderá tomar para conseguir limpar seu site o mais rapidamente possível. Mas antes de qualquer coisa vamos ver algumas considerações quanto à estrutura de sites em WordPress.
O Wordpress possui uma estrutura padrão também chamado como: ***"core"*** esse *core* são arquivos padrões que praticamente nunca mudam (a não ser de uma versão do Wordpress para outra).
Vou apresentar então a estrutura padrão do WordPress e quais são os arquivos e estruturas que praticamente nunca mudam:



Acima na imagem você pode observar que tirando a pasta **wp-content** e o arquivo **wp-config.php** (além do arquivo **.htaccess** caso esse existir) que estão riscados todos os outros arquivos são considerados arquivos *core* do WordPress, ou seja, são arquivos que por padrão não são modificados... a não ser se seu site tiver sido invadido, isso porque quando ocorre uma invasão em algum site WordPress essa invasão pode se duplicar e se esconder dentro de algum arquivo ou pasta padrão do Wordpress além, é claro, dos arquivos **.htaccess**, **wp-config.php** e dentro da pasta e subpastas do diretório **wp-content.**

- **Verifique se há algum arquivo modificado recentemente:**
  Como mencionamos anteriormente, os arquivos *core* de seu computador nunca mudam, a não ser de versão para versão ou caso o site em si tenha sido invadido. Então, através de um usuário de FTP (como por exemplo o Filezilla) ou então através do acesso **SSH** você

conseguirá verificar se algum arquivo do *core* de seu site foi modificado recentemente e se caso encontre algum que tenha sido modificado a pouco tempo recomendamos você a realizar uma análise minuciosa visando encontrar algum script adicionado ao arquivo padrão de seu site.

Bom, tirando os arquivos *core* de seu site os arquivos dentro da pasta **wp-content/** são arquivos que, durante a utilização/manutenção/criação de seu site vai estar em constante alteração. No entanto caso você tenha um site onde nem você nem mais outra pessoa tenha feito alguma alteração através do Dashboard do Wordpress (Painel Administrativo do site WordPress) isso implicaria que os arquivos que estão dentro da pasta **wp-content/** e demais subpastas também não devem ter em seu histórico algum indício de modificação recente.

Caso encontre algum arquivo dentro da **wp-content/** que tenha uma criação/modificação recente, tendo em vista de que ninguém tenha alterado nada no site, é um forte indício de que pode ter algo de errado nesses arquivos. Um outro lugar que comumente eles gostam de criar arquivos com scripts maliciosos é dentro da pasta **wp-content/uploads** então caso encontre algum arquivo criado ou modificado recentemente dentro dessa pastas e demais subpastas ou ainda encontre algum arquivo com extensão de scripts (.php, .json ou .js) é bem provável que seja algum arquivo malicioso, assim, o ideal é você analisar o conteúdo do arquivo para tentar identificar possíveis scripts maliciosos.

- **Identifique se os arquivos principais/padrões/*core* foram comprometidos:**
  Conforme mencionado acima, os arquivos *core* do Wordpress **nunca mudam** (a não ser de uma versão do WordPress para outra). Uma forma bastante eficaz de identificar se sua invasão adicionou algum *script* adicional em algum arquivo padrão do WordPress seria realizando uma comparação entre arquivos! (Atenção para realizar essa comparação com os arquivos *core* da mesma versão do WordPress). Essa verificação busca verificar a **integridade dos principais arquivos do Wordpress**.
  Para realizar essa verificação de seu site recomendamos que você baixe todos os arquivos de seu site para seu computador usando algum software de FTP, como por exemplo o Filezilla.

  Então, pensando que os arquivos *core* do Wordpress nunca mudam (a não ser de uma versão do WordPress para outra) uma forma bastante eficaz de identificar se sua invasão adicionou algum *script* adicional em algum arquivo padrão do WordPress seria realizando uma comparação entre arquivos!
  Essa comparação pode ser feita de algumas formas:
  - Comparação manual, arquivo por arquivo, se atentar à versão do WordPress de seu site. Caso você não saiba qual é a versão do WordPress de seu site basta ir no arquivo **wp-includes/version.php** e anotar a versão do WordPress do site invadido. Com o número da versão em mãos você pode acessar o site do WordPress e baixar a mesma versão do site invadido (para fazer o download de uma versão específica basta acessar: https://br.wordpress.org/download/releases). Após feito o download da versão limpa do Wordpress, baixada no site do Wordpress passaremos então pro próximo passo.
  - Comparação dos arquivos através de ferramentas de comparação. Para isso você pode utilizar uma ferramenta online a Diffchecker, caso queira realizar essa comparação com um programa instalado em seu computador você pode utilizar o software Winmerge ou caso queira realizar essa comparação utilizando SSH ou

através de linha de comando (no linux) você pode usar a seguinte linha de comando:

```
diff -r wordpress-limpo/  site-infectado/ -x wp-content
```

onde a pasta **wordpress-limpo/** é a pasta com os arquivos padrões que você baixou no site do Wordpress e a pasta **site-infectado/** é a pasta onde contém os arquivos do site infectado.

Uma outra opção, caso não queria-se comparar os arquivos que compõem o *core* do WordPress seria substituir os arquivos do core pelos arquivos padrões (baixados no site do WordPress). Fazendo isso você não precisará realizar a comparação, arquivo a arquivo, dos arquivos core do seu site, faltando então apenas a análise dos arquivos que não compõe o *core* do WordPress que seriam todos os arquivos que estão dentro da pasta **public/** e que fogem da estrutura padrão (ver imagem acima) além dos arquivos **.htaccess, wp-config.php** e demais arquivos dentro da pasta **wp-content/**.

Para os arquivos que fogem à normalidade, arquivos que não compõem a estrutura padrão do Wordpress, você precisará analisar manualmente o conteúdo dos mesmos para garantir que dentro deles não tenham nenhum script malicioso. Caso não tenha conhecimentos de programação ou não se sinta seguro em fazer essa verificação, recomendamos que você contrate um programador ou um especialista em limpeza de sites para realizar esses procedimentos.

Bom, agora que você já verificou/comparou e/ou substitui todos os arquivos das pastas *core* do WordPress vamos passar então para algumas verificações padrões da pasta **wp-content/**. Essa pasta, como comentado anteriormente, é um local onde não existe exatamente um padrão, pois é onde ficam os arquivos, plugins, imagens, backups, arquivos de cache e etc. Com isso, essa é, na maioria dos casos, a porta de entrada da invasão de seu site.
Assim, cada arquivo dentro desse diretório é onde deverá ser dado uma atenção maior na análise dos diretórios e arquivos que ali estão.

Dentre as pastas que estão dentro da pasta **wp-content/** está o diretório **uploads/**, é dentro desta pasta que serão adicionados os arquivos que são “upados” através de seu site. Na pasta **uploads/**, normalmente, devem constar apenas arquivos de mídias como arquivos de imagem, vídeos e áudios, porém **JAMAIS** arquivos de script como arquivos .js ou .php. Algumas das invasões de sites escondem alguns scripts exatamente dentro dessa pasta **uploads/** já que essa pasta por padrão permite que seus arquivos sejam acessados de forma pública.
Então, você precisará realizar essa varredura minuciosa em busca dos arquivos de script (.js ou .php) de forma manual (usando o FTP) ou através do acesso SSH utilizando o comando **find:**

```
find uploads/ -name "*.js" && find uploads/ -name "*.php"
```

Limpando manualmente os arquivos de plugin e tema do WordPress hackeados:

Como mencionado anteriormente, às vezes a invasão acontece por alguma vulnerabilidade de algum plugin ou tema. Isso porque ás vezes o plugin pro (pago) ou tema pro (pago)

craqueado (nulled) foi instalado em seu site e dentro dele havia algum *backdoor* culminando na invasão de seu site. Outras vezes a invasão é por intermédio de alguma vulnerabilidade de seu tema ou plugin free (de graça) e que foi explorada por algum atacante.

Independente dos motivos que levaram seu site a ser invadidos, quando você se deparar com seu site invadido você também conseguirá realizar a limpeza manual de seus arquivos de plugins e temas. Para isso você precisará fazer o download da cópia "limpa" de todos os seus plugins seja através do site do Wordpress (https://br.wordpress.org/plugins/) ou através do site oficial do plugin em questão e após baixado "subir/upar" a pasta, já descompactada, do plugin (por algum programa de FTP, sFTP ou ainda através do próprio painel da hospedagem) para a pasta **wp-content/plugins**. Lembre de excluir a pasta antiga do plugin existente na hospedagem antes de upar o plugin (já descompactado em seu computador) para a pasta da hospedagem.
O mesmo ocorre para seus temas, bastando que o cliente faça o download do tema através do site do Wordpress (https://br.wordpress.org/themes/) ou do site oficial do thema, extrair/descompactar em seu computador os arquivos e então "subir/upar" a pasta já descompactada (por algum programa de FTP, sFTP ou ainda através do próprio painel da hospedagem) para a pasta **wp-content/themes**. Lembrando de excluir a pasta antiga do tema existente na hospedagem antes de upar a pasta do tema.

OBS 1: Caso algum dos plugins ou do tema seja personalizado, ou seja, tenha sido desenvolvido sob encomenda ou sob demanda o ideal é realizar uma inspeção minuciosa, arquivo por arquivo, para identificar scripts maliciosos caso não seja possível baixar uma versão limpa desse tema ou plugin.
OBS 2: É extremamente importante não se basear apenas em análise de sites de buscas ou plugins de segurança como **Wordfence, Sucuri Scan** ou ainda o **MalCare** isso porque mesmo eles informando que seu site está 100% limpo pode ser que seu site ainda possua alguns resquícios da invasão. Isso acontece pois além da constante evolução as invasões e tipos de invasões não possuem um padrão e estão constantemente mudando sua forma de agir e variando e refinando seu *modus operandi* fazendo com que um plugin não substitua uma análise manual e criteriosa em seu site.

- **Malware em seu Banco de Dados:**
  Algumas vezes a infecção de seu site cria scripts dentro de Banco de Dados fazendo com que sua limpeza se torne um pouco mais desafiadora. No entanto, limpar arquivos de seus plugins, temas e bancos de dados é um passo essencial.

  Para identificar e remover malware em seu Banco de Dados você precisará primeiramente acessá-lo, você poderá acessar seu Banco de Dados através do PHPMyadmin, HeidiSQL, Workbench ou qualquer outro SGBD. Uma vez conectado ao seu banco de dados você deverá fazer um backup de seu Banco de Dados em formato .sql. Após realizado o backup do Banco de Dados você deverá pesquisar em todas as tabelas do seu banco de dados por conteúdo suspeito (palavras chaves como: **spammy, base64_decode, gzinflate, preg_replace, str_replace e etc…** ou algum outro link estranho). Em sua busca caso encontre alguma dessas palavras ou links suspeitos você poderá remover manualmente esse conteúdo e qualquer outro conteúdo suspeito visando limpar seu banco de dados.

Além disso, algumas vezes quando o site é invadido você notará através de buscas no Google (vá no Google e pesquise por: **site:seudominio.com** e algumas vezes você encontrará diversas páginas/artigos com conteúdos maliciosos indexados. Em casos assim, o ideal é mover essas postagens/páginas para o lixo visando não deixar nenhuma injetada, através da invasão, em seu site.
Para mover essa postagens do WordPress para o lixo basta alterar o campo de **post_status** da tabela de posts (normalmente o nome dessa tabela é **wp_posts**) para "trash" como na imagem abaixo:

Ou até mesmo excluir/apagar essa publicação de seu Banco de Dados.

Outra coisa que deve-se observar no Banco de Dados de um site invadido é se existe algum usuário (tabela **wp_users**) com o nome ou email suspeito, caso exista você poderá excluí-lo/apagar de seu Banco de dados.

- **Encontre e remova backdoors ocultos:**
Os hackers geralmente deixam um *backdoor* que lhes permite recuperar o acesso ao seu site WordPress. Os *backdoors* podem vir em uma variedade de formas e tamanho diferentes, e você pode encontrar facilmente mais de um tipo de *backdoor* em um site hackeado.

  Na grande maioria das invasões dos sites são adicionados um script dentro de um ou mais arquivos do site que tem a função de ser uma porta de entrada para uma invasão posterior ou uma re-infecção também conhecidos como ***backdoors***.Por isso, assim que você descobrir que seu site foi invadido é extremamente importante encontrar esses arquivos infectados e realizar a exclusão através de uma análise mais minuciosa nos arquivos dentro da pasta **wp-content/** ou ainda nos arquivos **index.php** e **wp-config.php** que estão dentro da pasta raiz de seu site.
  Normalmente os arquivos que contêm esses scripts *backdoors* maliciosos utilizam algumas das funções PHP a seguir:
  - base64
  - exec
  - move_uploaded_file
  - str_rot13
  - gzuncompress
  - eval
  - stripslashes

- system
- assert
- preg_replace (com /e/)

OBS: Nem todo arquivo que possui um dessas funções acima são necessariamente infectados uma vez que alguns plugins utilizam uma ou mais funções acima para realizar suas operações normais e legítimas de plugins.

- **Remova seu site da lista de bloqueio/Blocklist ou Blacklists:**
  Google, Avira, McAfee, Norton, Netcraft e outras empresas de segurança tem uma forma específica para verificar se um site é malicioso ao usuário que está acessando ou não. Uma vez que seu site foi invadido e continuou em execução pode ser que seu site possa ser adicionado em um dessas *blacklists*. Para isso, normalmente você precisará acessar o site dessas e preencher algum formulário ou mesmo entrar em contato solicitando a revisão da decisão ou para que seu site seja retirado mediante alguma vistoria por parte deles.

  Quando seu site foi invadido a Umbler fazemos a suspensão de seu site para evitar que seu site fique ativo e você seja penalizado posteriormente sendo adicionado a alguma Blacklist por exemplo. No entanto, caso você já tenha feito a limpeza de seu site você pode nos solicitar seja via suporte para que removamos a suspensão de seu site. **É de extrema importância que você nos forneça detalhes de como você removeu o malware para que possamos analisar e realizar a remoção do bloqueio de seu site.**

Dicas de Segurança e Dicas para se Prevenir seu site de Invasões:

- **Tenha sempre backups periódicos:**
  Os backups não são garantia de que seu site não será invadido já que você pode ser invadido e só um tempo depois notar isso. No entanto, ele pode ser de grande ajuda quando você precisa, por exemplo, saber quando que essa invasão ocorreu. Além disso os backups é uma forma mais fácil de você voltar seu site até um estado onde ele não estaria invadido, dando-lhe tempo para analisar a estrutura invadida e corrigi-la sem deixar seu site fora do ar.

- **Exclua componentes não utilizados:**
  Um componente (plugin ou tema) não utilizados pode ser uma porta de entrada para atacantes. Mantenha sempre um backup de trabalho para restaurar facilmente em caso de problemas.

- **Mantenha seu site atualizado:**
  É extremamente importante atualizar todos os plugins, temas e o próprio WordPress atualizado, pois muitas das atualizações lançadas corrigem uma ou várias vulnerabilidade descobertas que podem levar seu site a ser invadido.

- **Não instalar plugins ou temas crackeados, nulled ou de fonte duvidosa:**
  Os plugins ou temas crackeados, também conhecidos como nulled são plugins onde foram adicionados novos códigos ao código fonte original do tema ou plugin, no entanto ninguém sabe quais foram esses códigos adicionados. Então um ou mais código adicionado, de forma oculta, pode estar abrindo uma brecha para a invasão ou ainda sendo o causador da invasão em seu site!

- **Procure manter as permissões de arquivos e pastas o recomendado pelo próprio time do Wordpress:**
  Na documentação do próprio Wordpress ele coloca algumas recomendações sobre as permissões ideais tanto para arquivos e para as pastas de seus site Wordpress. No artigo do Wordpress eles mencionam que as permissões ideais para:
  - Arquivos é a permissão **644**;
  - Pastas é a permissão **755;**

- **Altere suas senhas e não use senhas fáceis:**
  Alterar suas senhas sejam elas do painel administrativo de seu site, de seus usuários FTP ou usuários SSH, Banco de Dados ou ainda de seu Painel do Usuário da Umbler. Além disso as senhas utilizadas devem ser senhas complexas, então nada de senhas do tipo “12345678”, “senha123” ou algo similares isso porque são senhas que comumente são utilizadas por outros usuários, o que pode ser uma falha gravíssima de segurança. Então considere utilizar senhas de no mínimo 12 caracteres contendo caracteres especiais, letras maiúsculas e minúsculas além de números.

- **Por mais raro que pareça (mais nem tanto) a invasão possa partir do seu computador:**

Bom, por mais improvável que possa parecer, algumas vezes a invasão de nossa aplicação pode ser originária do computador de acesso a seu site. Isso pode acontecer, por exemplo, caso seu computador esteja com algum vírus e você o utilize para acessar seu site através de um **programa de FTP**, através do SSH ou ainda somente acessar o dashboard de seu site. Acontece pois algumas vezes o vírus presente no computador de acesso seja de algum tipo que monitora tudo que é digitado, ou faz algum tipo de captura ou sua replicação em vários ambientes diversos (seu computador e a hospedagem de seu site por exemplo).
Por isso é importante manter o computador que você utiliza para acessar sua hospedagem sempre limpo de ameaças (trojan, keylogger ou outros tipos de vírus) e sempre com o antivírus em dia.

- **Utilize algum plugin de segurança e configure-o bem:**
  Plugins de segurança criam uma certa “defesa” acerca de seu site **e pode ajudar** a mitigar ataques mais comuns como: DDoS, exploração de vulnerabilidades, ataques de força bruta e algumas outras ameaças.