POR UM WORDPRESS MAIS SEGURO...

Flávio Silveira - WordCamp Curitiba 2012

Quem sou...

- Especialista??
- Web / Cultura
- Games.
- Comunidade PHP.
- Tecnologia.

Porque se preocupar...

- Conteúdo.
- Seu tempo.
- Confiança.
- Seu site nos sites de busca.
- Prejuízos.

Porque se preocupar...

Invasão de hackers ao site do Bike Tour prejudica inscrições de ciclistas

Evento acontece no aniversário de São Paulo, no dia 25 de janeiro.
Organização irá enviar e-mail com orientações para os prejudicados.

Do G1 SP

imprimir

Uma invasão de hackers ao site do Bike Tour fez com que milhares de pessoas que se inscreveram para o evento não conseguissem efetuar o pagamento da taxa de inscrição. Segundo a organização, cerca de 5.500 ciclistas foram afetados pela invasão.

Quem conseguiu se inscrever, mas não pôde pagar a taxa de R$ 180, não precisa se preocupar. A organização do evento informou que irá enviar um e-mail com as orientações sobre como deverá ser feito o pagamento.

A terceira edição do Bike Tour, como de costume, acontece no aniversário de São Paulo, no dia 25 de janeiro. A largada será feita na Ponte Octávio Frias de Oliveira, mais conhecida como ponte estaiada.

Porque se preocupar...

Serviço de blog gratuito Wordpress sofre invasão de hackers

Criminosos conseguiram acesso total ao site.
Troca de senha é recomendada para os usuários.

Altieres Rohr
Especial para o G1

imprimir

Criminosos ganharam 'acesso root', afirmou responsável pelo serviço (Foto: Reprodução)

Invasores conseguiram acesso total a "vários servidores" do serviço de blogs **Wordpress**, de acordo com um comunicado escrito por Matt Mullenweg, responsável pelo serviço. "Potencialmente qualquer coisa nesses servidores pode ter sido revelada", escreveu. A Automattic, que opera o serviço, ainda está investigando como a invasão ocorreu e quais dados podem ter sido revelados, mas afirma já ter tomado medidas para prevenir novos incidentes.

Nas palavras Mullenweg, os atacantes conseguiram "acesso root". "Root" é o nome do usuário administrador de sistemas Unix, normalmente usado em servidores, e é capaz de realizar qualquer tarefa no sistema. De acordo com as estatísticas do próprio Wordpress.com, o serviço hospeda 19 milhões de blogs.

Códigos do software usado no site teriam sido expostos. Boa parte do Wordpress é código aberto e está disponível para download na internet, mas códigos próprios do Wordpress, que

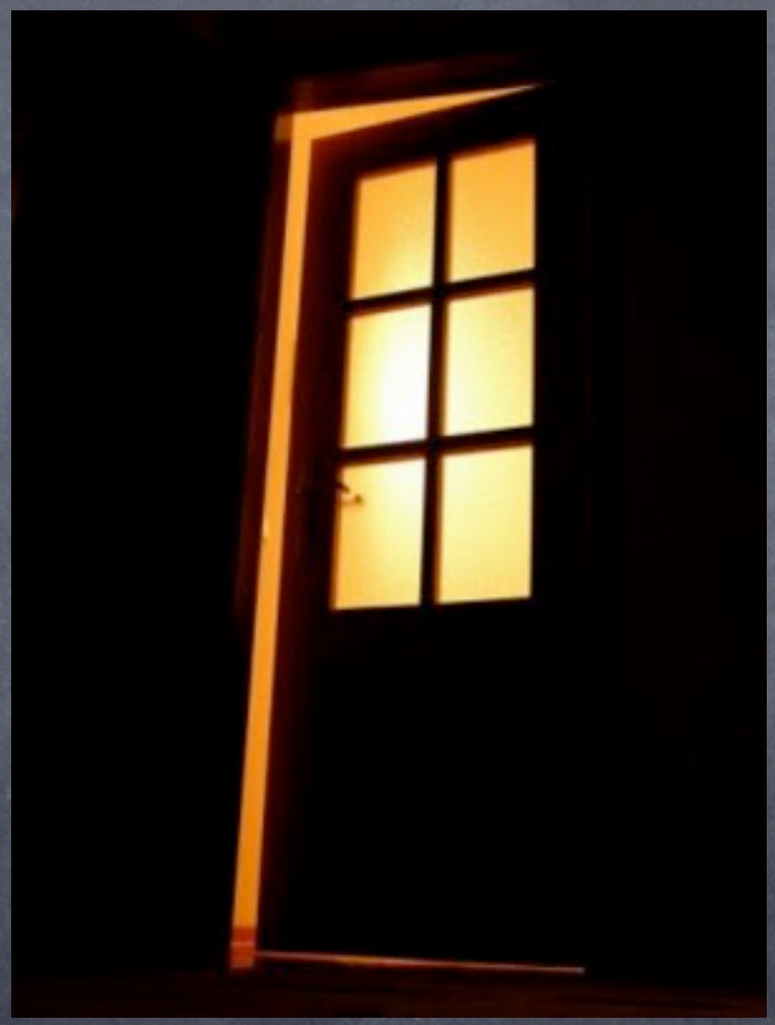
Mais do mesmo...

WHILE (problemas de segurança)
{

- Artigos;
- Temas de palestras mundo afora;

}

Segurança...



Segurança...

Básico...

- Mantenha seu wordpress atualizado.
- Seus plugins também.
- Elimine plugins que você não utiliza mais.

Não mostre sua versão...

```
▼<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US">
  ▼<head profile="http://gmpg.org/xfn/11">
      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
      <title>Flávio Silveira  </title>
      <meta name="generator" content="WordPress 3.3.2">
      <!-- leave this for stats -->
```

- Altere o header.php do seu tema.

```
▼<html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US">
  ▼<head profile="http://gmpg.org/xfn/11">
      <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
      <title>Flávio Silveira  </title>
      <!-- leave this for stats -->
```


WordPress
Username
Password
Remember Me
Log In


WordPress
Username
admin
Password
Remember Me
Log In

Login Padrão...

Login Padrão...

Login Padrão...

- Direto no Banco de dados.
- Criando novo usuário

Senha...

Senha...

- Senha não é para ser fácil de lembrar.
- Não faça uso da mesma senha para vários serviços.
- Não guarde senhas em emails ou arquivos.

Dicas para criar senhas...

Palavra -> dicionário

Dicas para criar senhas...

Palavra -> dicionário

Letras ->

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Números ->

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas ->

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas -> d9c3N5r8

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas -> d9c3N5r8

Símbolos ->

Dicas para criar senhas...

Palavra -> dicionário

Letras -> d c n r

Números -> d9c3n5r8

Maiúsculas -> d9c3N5r8

Símbolos -> d*c3N5r8#

Dicas para criar senhas...

Facebook -> F B

Dicas para criar senhas...

Facebook -> F B

Git Hub ->

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Vimeo ->

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Facebook ->

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Facebook -> 1 7

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Facebook -> 1 7

Orkut ->

Dicas para criar senhas...

Facebook -> F B

Git Hub -> G H

Vimeo -> V M

Facebook -> 1 7

Orkut -> 0 9

Senha...


New Password
••••••••••
••••••••••
If you would like to change the passwor
Type your new password again.
Strong
Hint: The password should
stronger, use upper and lo

Múltiplas tentativas...

Plugin: Login LockDown

Não mostre os erros...


```
add_filter('login_errors', create_function('$a', 'return null;'));
```

Login SSL...

- Confira se sua hospedagem tem suporte.
- Em wp-config.php, adicione:

```
define('Force_SSL_ADMIN', true);
```

- Plugin: SemiSecure Login.

Permissões...

- Sempre após instalar sete as permissões adequadas para suas pastas.

Pastas	755
Arquivos	644

- Começe com as permissões acima, altere se necessário.
- Pode variar de acordo com a configuração do servidor.

Mova seu wp-config...

- Desde a versão 2.6 do wordpress, você pode mover seu wp-config um diretório acima.

/www/meu_blog/wp-config.php

mova para

/www/wp-config.php

- O wordpress checa o diretório pai automaticamente se não encontrá-lo na raiz da instalação.

Htaccess e wp-config...

- Proteja o arquivo que tem suas configurações de banco de dados.

```
<files ~ "^\.(htaccess)$">
   deny from all
</files>

<files wp-config.php>
   order allow, deny
   deny from all
</files>
```

Robôs de sites de busca...

- robots.txt

```
Disallow: / wp-*
```

Listagem de arquivos...

- wp-content

Name	Last modified	Size	Description
Parent Directory		-	
2009/	29-Mar-2011 11:48	-	
2010/	29-Mar-2011 11:49	-	
2011/	30-Nov-2011 18:31	-	
2012/	31-May-2012 19:29	-	

- .htaccess

```
Options All -Indexes
```

Prefixo do banco de dados...

- Antes de instalar seu wordpress, altere o arquivo wp-config.php.

```
$table_prefix = ‘O_que_vc_quiser_’;
```

Prefixo do banco de dados...

Para quem já instalou

- Altere o arquivo wp-config.php
- Dê um rename nas tabelas do banco de dados.
- Na Tabela _options mudar no registro option_id 94 o prefixo wp_user_roles.
- Na tabela _usermeta alterar as meta keys wp_capabilities e wp_user_level.

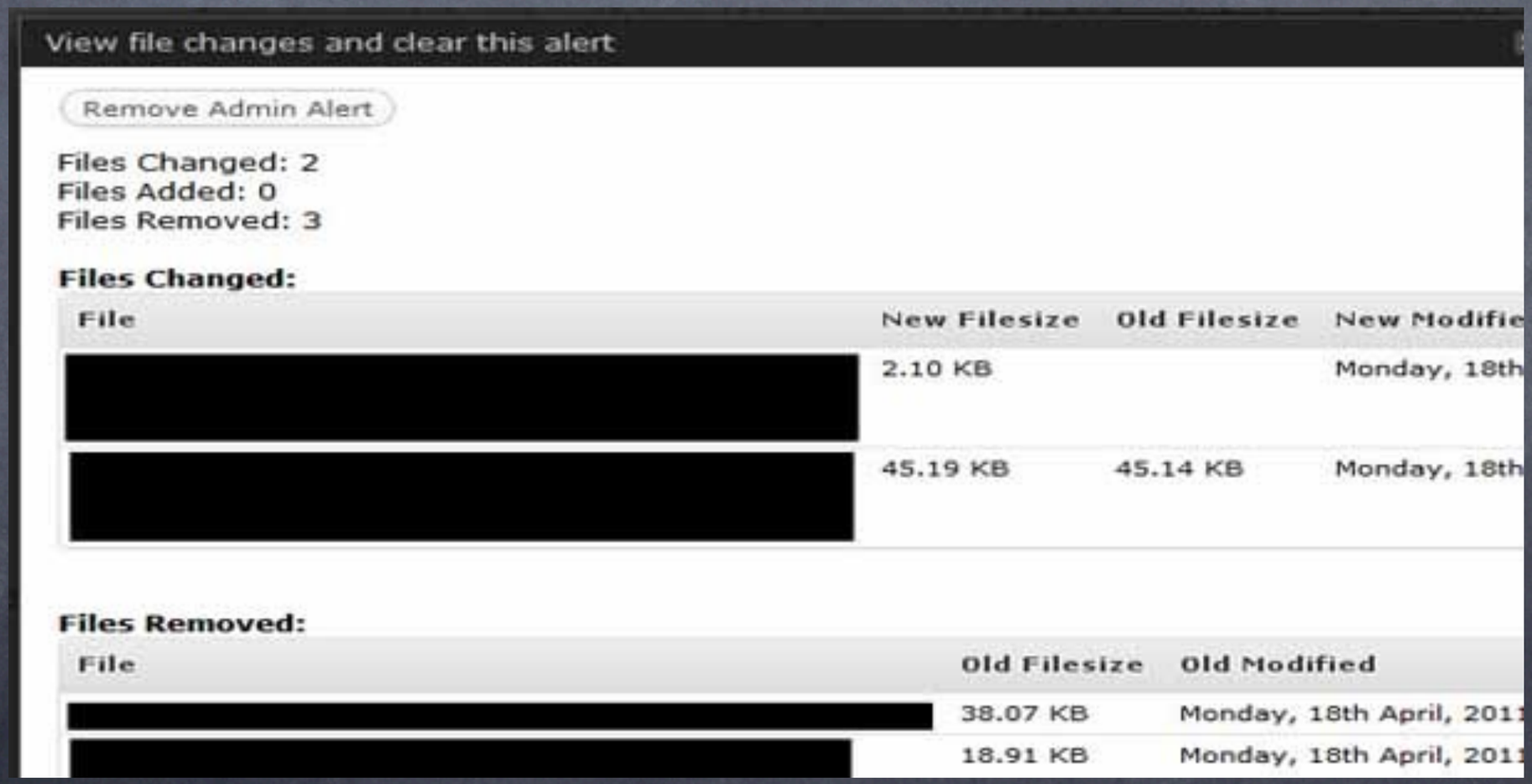
Plugins...

Plugins já comentados

- Login LockDown.
- SemiSecure Login.

Plugins...

Wordpress File Monitor



Plugins...

Wordpress Security Scan

Resumindo...

Referências...

- Lucas Peperaio http://www.lucaspeperaio.com.br
- Syed Balkhi http://www.balkhis.com
- Brad Willians (WordCamp NY)

Contato...

- Site -> http://www.flaviosilveira.com
- Twitter -> @flaviosilveira
- Email -> flavioaugustosilveira@gmail.com
- Php Curitiba

Obrigado!