Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

SHADOWCAPTCHA EXPLOTA WORDPRESS PARA DISTRIBUIR MALWARE, INCLUYENDO RANSOMWARE Y CRIPTOMINEROS

26/ 08 / 2025

CONTENIDO

INTRODUCCIÓN

ShadowCaptcha es una campaña cibercriminal que ha comprometido más de 100 sitios basados en WordPress. Los atacantes redirigen a los usuarios a captchas falsos, engañándolos para que instalen malware en sus dispositivos, como stealers, cryptominers o incluso ransomware.

SHADOWCAPTCHA EXPLOTA WORDPRESS PARA DISTRIBUIR MALWARE, INCLUYENDO RANSOMWARE Y CRIPTOMINEROS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_08_26_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	26/08/2025
Es día cero (0 day):	No

RESUMEN

ShadowCaptcha es una campaña cibercriminal que ha comprometido más de 100 sitios basados en WordPress. Los atacantes redirigen a los usuarios a captchas falsos, engañándolos para que instalen malware en sus dispositivos, como stealers, cryptominers o incluso ransomware.

¿Cómo funciona ShadowCaptcha?

El ataque comienza cuando un usuario visita un sitio web de WordPress infectado. Un JavaScript malicioso inicia una cadena de redireccionamientos hacia una página que simula ser un captcha de Cloudflare o Google.

Cuando la víctima realiza lo que parece un paso normal (hacer clic o seguir una instrucción), es guiada a ejecutar acciones peligrosas, como abrir el diálogo "Ejecutar" de Windows o guardar y ejecutar un archivo .HTA con mshta.exe.

Técnicas para aumentar la efectividad

Los cibercriminales utilizan varias técnicas para hacer el ataque más elaborado:

- Ingeniería social "ClickFix": Una táctica visual que engaña al usuario para que ejecute comandos sin darse cuenta.
- JavaScript ofuscado: Copia comandos al portapapeles (navigator.clipboard.writeText) sin la interacción directa del usuario.
- Técnicas anti-debugging: Complican el análisis del malware por parte de los investigadores.

Funciones avanzadas del malware

En algunos casos, ShadowCaptcha instala un minero de criptomonedas basado en XMRig. El malware descarga la configuración de Pastebin, lo que facilita su ajuste en tiempo real.

También puede desplegar un driver vulnerable, WinRing0x64.sys, para obtener acceso a nivel del kernel y optimizar el uso del CPU para minar de forma más eficiente.

Otro hallazgo crítico: CVE-2025-54049

Además de esta campaña, se descubrió una vulnerabilidad de asignación incorrecta de privilegios (CWE-266) en el plugin Custom API for WP de miniOrange.

Esta falla, que afecta a todas las versiones hasta la 4.2.2, permite que usuarios con privilegios mínimos escalen hasta el control total del sitio sin necesidad de interactuar con el administrador. Se le ha otorgado una criticidad de 9.9.

¿Cómo funciona el ataque?

Un atacante con acceso básico o un actor remoto puede abusar del error de asignación de permisos para ejecutar acciones privilegiadas dentro de WordPress, como:

- Modificar contenido o configuraciones.
- Otorgarse a sí mismo el rol de administrador.
- Comprometer plugins y temas.

El ataque puede realizarse de forma remota y sin interacción del usuario, lo que lo hace extremadamente peligroso en sitios públicos.

RECOMENDACIONES

- Actualiza siempre WordPress y sus plugins a las versiones más recientes.
- Activa la autenticación multifactor (MFA) para las cuentas de administrador.
- Aplica segmentación de red para limitar el alcance de un ataque.
- Educa a los usuarios: Advierte que no deben realizar captchas fuera del navegador ni ejecutar comandos o archivos descargados de páginas web sospechosas.
- Supervisa tu sitio con un WAF (Web Application Firewall) para detectar redireccionamientos o scripts inusuales.
- Instala la versión 4.2.3 o superior del plugin Custom API for WP.
- Utiliza roles mínimos para los usuarios, bloquea las instalaciones directas de plugins y monitoriza los cambios.

NOTICIA COMPLETA

https://devel.group/blog/shadowcaptcha-explota-wordpress-para-distribuir-malware-incluyendo-ransomware-y-criptomineros/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group