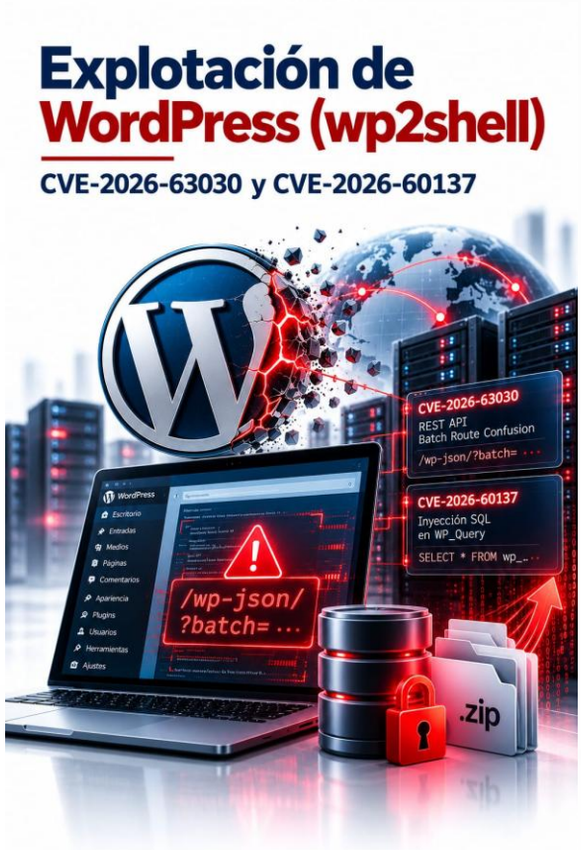
Alerta

Explotación Kapibala_wp2shell_WordPress

COLCERT AL – 20260928 - 120

TIC

1. Resumen Ejecutivo



Se identificó una campaña activa y altamente automatizada del actor de amenazas conocido como *Kapibala* (vinculado en diversos análisis al clúster Red Heron, presuntamente de origen chino), el cual despliega la cadena de exploits wp2shell contra servidores WordPress expuestos a internet. *El ataque se fundamenta en la explotación encadenada de dos vulnerabilidades críticas:* la CVE-2026-63030 (confusión de rutas en la API REST), que permite eludir los controles de autenticación, y la CVE-2026-60137 (inyección SQL no autenticada en la clase WP_Query), que habilita la extracción de bases de datos o la ejecución remota de código. Paralelamente, este actor explota la vulnerabilidad CVE-2026-7273 en equipos ZyXEL GS1900 para comprometer la infraestructura de red.

Tras obtener el acceso inicial, el atacante instala web shells persistentes en rutas públicas de la raíz web, crea cuentas de administrador ilegítimas bajo el dominio de la víctima y altera sus fechas de registro (mediante la técnica de timestomping) para dificultar el análisis forense. Durante la investigación, se identificaron más de 17 variantes de scripts diseñadas para evadir el AMSI, suplantar tokens (token impersonation) y volcar las credenciales del registro y la base SAM. El patrón de desarrollo acelerado de estas herramientas, sumado a la presencia de comentarios en chino, sugiere un uso intensivo de Inteligencia Artificial (LLM/IA) para la creación de los artefactos maliciosos. En la fase final, el actor busca credenciales en archivos de configuración como wp-config.php, ejecuta ataques de password spraying contra el motor SQL y ha logrado exfiltrar —en incidentes analizados a nivel global— paquetes con más de 18.000 credenciales en texto plano mediante solicitudes HTTP simples.

NIVEL DE RIESGO

ALTO

Esta campaña tiene un alcance global (afectando a más de 29 países) y Colombia está confirmada dentro de sus objetivos estratégicos. Mediante el monitoreo de la superficie de ataque, se identificaron activos comprometidos en estado Abierto/Confirmado pertenecientes a *los sectores de Gobierno, Salud y Educación.* Dado el nivel de exposición confirmado sobre la infraestructura nacional, el uso de técnicas de evasión avanzadas y la capacidad demostrada de exfiltración masiva de datos sensibles, esta amenaza se clasifica con un nivel de criticidad **ALTO**.

En consecuencia, se recomienda a las entidades verificar con urgencia su versión de WordPress, aplicar el parcheo inmediato de las CVE involucradas y revisar cualquier indicio de compromiso (como cuentas de administrador no reconocidas o presencia de *web shells*) como acción prioritaria.

Contexto de la Amenaza

El actor de amenazas conocido como Kapibala despliega activamente la cadena de exploits wp2shell para comprometer servidores web basados en WordPress. Este vector de ataque combina una vulnerabilidad de confusión de rutas en la API REST (CVE-2026-63030) con una inyección SQL no autenticada (CVE-2026-60137), lo que permite a los atacantes instalar web shells persistentes y exfiltrar bases de datos con información sensible. Como agravante regional, los análisis confirman que Colombia se encuentra explícitamente dentro de los objetivos estratégicos de este actor.

Técnicas y Tácticas – MITRE ATT&CK

A continuación, se detalla el conjunto de tácticas, técnicas y procedimientos (TTPs) identificados durante el análisis técnico, alineados con el marco de referencia global MITRE ATT&CK.

Táctica	Técnica / Subtécnica	Descripción / Detalle
Acceso Inicial	T1190 – Exploit Public-Facing Application	Explotación de vulnerabilidades públicas en WordPress (wp2shell / CVE-2026-63030 y CVE-2026-60137).
Ejecución	T1059.001 – Command and Scripting Interpreter: PowerShell	Ejecución de comandos mediante PowerShell para descarga e instalación de payloads, y para el empaquetamiento y almacenamiento de información sustraída en archivo ZIP.
Persistencia	T1505.003 – Server Software Component: Web Shell	Implantación de web shells persistentes en el servidor de aplicaciones web.
Persistencia	T1136.001 – Create Account: Local Account	Creación ilegítima de cuentas administradoras dentro de WordPress.
Sigilo	T1027 – Obfuscated Files or Information	Uso de variaciones complejas de código y scripts posiblemente generados/optimizados mediante IA para eludir herramientas de seguridad.
Deterioro de la Defensa	T1685 – Disable or Modify Tools	Bypasses dirigidos contra Microsoft AMSI.
Sigilo	T1070.006 – Indicator Removal: Timestomping	Alteración de la fecha de registro del usuario administrador en la base de datos para dificultar el análisis forense.
Credenciales de Acceso	T1552.001 – Unsecured Credentials: Credentials In Files	Lectura de credenciales en texto claro almacenadas en archivos de configuración como wp-config.php.
Credenciales de Acceso	T1110.003 – Brute Force: Password Spraying	Ataques de password spraying dirigidos hacia servicios de base de datos internos.
Credenciales de Acceso	T1003 – OS Credential Dumping	Intentos de extracción de credenciales mediante el volcado de colmenas de registro/SAM.
Colección	T1560.001 – Archive Collected Data: Archive via Utility	Empaquetamiento y compresión de bases de datos sustraídas en formato .zip usando utilidades del sistema.
Exfiltración	T1041 – Exfiltration Over C2 Channel	Transferencia no autorizada de los archivos comprimidos mediante peticiones HTTP.

Cadena de Ataque (Kill Chain)

La secuencia de intrusión de la campaña Kapibala (wp2shell) se despliega en múltiples fases: inicia con el escaneo masivo de servidores WordPress expuestos a internet, continúa con la explotación encadenada de las vulnerabilidades CVE-2026-63030 y CVE-2026-60137 para consolidar un acceso no autorizado, y culmina con el establecimiento de persistencia asistida por Inteligencia Artificial (IA) junto con la exfiltración masiva de credenciales mediante solicitudes HTTP simples.

Vulnerabilidade involucradas

CVE	Descripción	Severidad	Efecto
CVE-2026-63030	WordPress REST API Batch Route Confusion	**Alta**	Permite evasión de controles de autenticación.
CVE-2026-60137	WordPress Unauthenticated SQL Injection (WP_Query)	**Alta**	Permite extracción de datos de la base de datos o RCE encadenado.
CVE-2026-7273	ZyXEL GS1900 CGI Buffer Overflow	**Alta**	Explotado paralelamente por el mismo actor para comprometer equipos de red.

Recomendaciones Técnicas

Las siguientes medidas preventivas y de mitigación se formulan a partir de las tácticas, técnicas y capacidades ofensivas descritas en las secciones anteriores

Contención y remediación

- Verificar la versión instalada en los CMS WordPress de la entidad y aplicar de inmediato los parches correspondientes a las vulnerabilidades CVE-2026-63030 y CVE-2026-60137. Si la actualización no es factible de forma inmediata, restringir el acceso a la API REST (/wp-json/) mediante políticas en el WAF o reglas a nivel del servidor web.
- Actualizar el firmware de los equipos ZyXEL GS1900 expuestos a internet para mitigar la CVE-2026-7273, o en su defecto, aislarlos de la exposición pública directa.
- Auditar la tabla de usuarios de WordPress (wp_users) en busca de cuentas de administrador no reconocidas por el equipo de TI que utilicen correos bajo el dominio propio, prestando especial atención a manipulaciones anómalas en el campo user_registered.
- Identificar y eliminar web shells alojadas en rutas públicas de la raíz web (tales como wp-content/uploads, plugins y temas) mediante herramientas de escaneo de integridad de archivos.
- Rotar las credenciales de bases de datos y de cuentas de servicio expuestas en archivos de configuración (wp-config.php), además de revisar los logs del motor SQL en busca de patrones asociados a password spraying.

Fortalecimiento de controles técnicos

- Habilitar un WAF (Web Application Firewall) implementando reglas específicas para bloquear la explotación de la API REST de WordPress y detectar patrones de inyección SQL en los parámetros de la clase WP_Query.

- Monitorear activamente la creación de archivos ZIP de gran tamaño mediante la ejecución de PowerShell en los servidores web, así como la generación de solicitudes HTTP salientes anómalas desde dicha infraestructura (lo cual constituye un indicador claro de exfiltración).

- Configurar alertas de seguridad ante cualquier ejecución de PowerShell en servidores IIS o Apache que alojen sitios WordPress, dado que el comportamiento habitual de estos servidores no incluye la invocación de intérpretes de scripting.

Fuentes

GreyNoise. (2026). Open Season on Kapibala: Attacker Steals Government Records via WordPress Exploitation.

https://www.greynoise.io/blog/open-season-on-kapibala-attacker-steals-government-records-wordpress-exploitation

The MITRE Corporation. (s. f.). MITRE ATT&CK®: Knowledge base of adversary tactics and techniques.

https://attack.mitre.org/