# Informe de Análisis de Ataque y Propuesta de Mejora de Ciberseguridad para Port Shool

Análisis y estrategias para la protección de la infraestructura digital.

**Autor:** Emanuel Sanchez.

Informe de Auditoría de Seguridad — Compromiso por troyano/adware en WordPress
Cliente: Port School
Empresa auditora: ARX Data
Fecha: 12 de Noviembre de 2025
Auditor principal: Equipo de Respuesta a Incidentes — Emanuel Sanchez

1. Resumen ejecutivo

Se detectó y mitigó un compromiso en un sitio WordPress consistente en un troyano con comportamiento de adware. El código malicioso fue introducido a través de un plugin comprometido y actuaba insertando/modificando contenidos (imágenes, archivos, vídeos), generando redirecciones y anuncios no autorizados, y exfiltrando credenciales. La intervención incluyó aislamiento de plugins mediante FTP, escaneos con Wordfence y Sucuri, eliminación de archivos infectados y fortalecimiento de controles de acceso. Este informe documenta hallazgos, acciones realizadas, impacto y recomendaciones técnicas y organizativas para prevenir reincidencias.

2. Alcance de la auditoría

- Plataforma auditada: Instalación WordPress (core, plugins, temas, directorios wp-content y sistema de archivos relacionado).
- Herramientas empleadas: Wordfence, Sucuri (site scanner), acceso FTP/SFTP para inspección/aisla revisión manual de archivos y permisos.
- Objetivo: identificar vector de entrada, alcance del compromiso, eliminar la amenaza y proponer medidas de recuperación y endurecimiento.

3. Metodología

1. Identificación y aislamiento: Se desconectaron (por FTP) plugins sospechosos y se puso el sitio en modo mantenimiento/limpieza para evitar mayor propagación.
2. Escaneo automatizado: Ejecución de Wordfence y Sucuri para detección de archivos modificados, firmas de malware y patrones maliciosos.
3. Análisis manual: Revisión de archivos PHP/JS modificados, búsqueda de código ofuscado (eval, base64_decode, gzuncompress, str_rot13, etc.), revisión de .htaccess, crons y nuevos usuarios.
4. Eliminación controlada: Eliminación/cuarentena de archivos infectados preservando integridad de componentes esenciales.

Remediación de accesos: Cambio de credenciales, activación 2FA, limitación de intentos de acceso, ajustes de firewall (Wordfence) y medidas de monitoreo.

4. Hallazgos (Resumen técnico)

4.1 Vector de entrada

- Origen: Plugin malicioso o plugin legítimo comprometido instalado/actualizado recientemente.
- Vulnerabilidad explotada: Posible ejecución de código mediante plugin con entradas no sanitizadas o archivos del plugin que contenían backdoor.

4.2 Comportamiento del malware

- Inserción/modificación de contenido (imágenes, archivos, vídeos) en wp-content/uploads y en entradas existentes.
- Inyección de scripts/iframes y redirecciones hacia contenido publicitario (adware).
- Recolección/exfiltración de credenciales (posible captura de formularios de login o envío de fichero de configuración).
- Persistencia mediante archivos ofuscados y modificaciones en .htaccess / cron jobs.
- Posibles puertas traseras en archivos de tema (functions.php) o en archivos de plugin.

4.3 Indicadores de compromiso (IOCs) observados

- Archivos PHP con uso inusual de base64_decode, eval, create_function, gzuncompress.
- Archivos con nombres similares a class-*.php o con timestamps recientes en wp-content/plugins/ y wp-content/uploads/.
- Entradas nuevas en crontab de PHP o tareas programadas que ejecutan scripts desde wp-content.
- Nuevas cuentas administrativas o modificaciones en permisos de usuarios.

- Registros de acceso (webserver) mostrando peticiones a URLs anómalas / solicitudes POST sospechosas.

(Nota: los IOCs concretos varían por sitio; se recomienda la búsqueda exacta en el entorno comprometido.)

5. Evaluación de impacto
   - Disponibilidad: El sitio fue degradado temporalmente por inserciones y por el modo de limpieza.
   - Integridad: Contenido del sitio fue alterado (archivos multimedia y páginas).
   - Confidencialidad: Riesgo real de exposición de credenciales de administradores, FTP/cPanel y posibles datos de usuarios.
   - Reputación: Riesgo de bloqueo por navegadores/anti malware y pérdida de confianza de usuarios.
6. Acciones ejecutadas (cronología resumida)
   1. Recepción del incidente y contención inicial: aislamiento de plugins sospechosos vía FTP.
   2. Escaneo completo con Wordfence y Sucuri: identificación de archivos infectados y revisión de la tabla `wp_users` en busca de usuarios administrador creados por el malware que no fueron detectados por los escaneos automáticos..
   3. Aislamiento/cuarentena de archivos maliciosos (separación a carpeta segura fuera de public_html).
   4. Eliminación controlada de código malicioso manteniendo archivos esenciales intactos.
   5. Restauración de versiones limpias cuando estuvo disponible y verificación de integridad del core.
   6. Cambio de contraseñas: WP admins, FTP/SFTP, cPanel, base de datos y cuentas de correo.
   7. Activación de 2FA para cuentas administrativas.
   8. Configuración de Wordfence: bloqueo de URL sospechosas, activación firewall de aplicación (WAF limitación de intentos de acceso al panel admin.
   9. Programación de escaneos periódicos y alertas por email.

Remediación técnica recomendada (acciones realizadas y pendientes) Inmediatas (P0)

- Eliminar/quarantena de todos los archivos identificados como maliciosos.
- Cambiar todas las credenciales comprometidas (WP admin, FTP, SFTP, cPanel, DB, cuentas de corr
- Activar 2FA para todos los administradores.
- Poner el sitio en modo mantenimiento hasta validar la limpieza.
- Restablecer permisos de archivos y carpetas (files: 644, dirs: 755) y asegurar propietario correcto (user del servidor web).
- Corto plazo (P1)
- Actualizar WordPress core, plugins y temas a sus versiones seguras.
- Eliminar plugins y temas no usados o de dudosa procedencia.
- Desactivar edición de archivos desde el dashboard (define('DISALLOW_FILE_EDIT', true);).
- Revisar y limpiar .htaccess y crons; eliminar entradas no autorizadas.
- Revisar usuarios y roles, eliminar cuentas desconocidas y reducir privilegios.
- Mediano plazo (P2)
- Implementar WAF a nivel de servidor (Cloudflare/WAF del proveedor o WAF gestionado) además de de Wordfence.
- Implementar monitorización de integridad (file integrity monitoring) y alertas en cambios de archivos críticos.
- Revisar logs (webserver, PHP, cPanel) para identificar el alcance histórico del exfiltrado.
- Realizar una copia limpia de la web en entorno de staging y pruebas de penetración focalizadas en plugins y endpoints administrativos.
- Largo plazo (P3)
- Definir ejercicio regular de revisión/seguridad (escaneos semanales automáticos y auditorías trimestrales).
- Políticas de instalación de plugins (lista blanca, aprobación previa, pruebas en staging).
- Formación al equipo en seguridad y respuesta a incidentes.

7. Comandos y búsquedas útiles (para el equipo técnico)

Ejemplos para localizar código sospechoso en el servidor (ejecutar desde la raíz del sitio, con privilegios apropiados):

```
grep -R --line-number -E "eval\(|base64_decode\(|gzuncompress\(|create_function\(" wp-content | less find . -type f -mtime -30 -name "*.php" -print
grep -R --line-number -E "<iframe|window.location|document\.location|location.href" wp-content | less
crontab -l -u www-data
```

(Ajustar www-data al usuario apropiado.)

8. Recomendaciones de endurecimiento (resumidas)
   - Mantener copias de seguridad periódicas y verificadas, especialmente antes de instalar/actualizar plugins.
   - Usar autenticación por llave para SFTP; restringir acceso FTP y deshabilitar FTP si es posible.
   - Aplicar principio de mínimo privilegio para cuentas y bases de datos.
   - Habilitar 2FA en todas las cuentas administrativas.
   - Forzar contraseñas fuertes y rotación periódica.
   - Deshabilitar XML-RPC si no se usa.
   - Monitorización continua: integridad de archivos, alertas de inicio de sesión, bloqueo por IP y logs centralizados (si es posible, SIEM básico).
   - Política de aprobación de plugins: sólo instalar plugins desde repositorios confiables, mantener un inventario y revisiones de seguridad previas en staging.
9. Plan de recuperación y monitorización
   1. Verificación post-limpieza: escaneo completo con Wordfence y Sucuri; revisiones manuales de archivos críticos (wp-config.php, .htaccess, functions.php, index.php).
   2. Restablecimiento controlado: restaurar desde backup limpio si existe (previo a la instalación del plugin comprometido).
   3. Monitoreo intensivo: escaneos diarios por 14 días y alertas inmediatas por actividad sospechosa.
   4. Reporte y lecciones aprendidas: documentar root cause, actualizar políticas y bloquear contar con un playbook de respuesta a incidentes.
   5. Conclusión

El incidente fue ocasionado por un plugin comprometido que actuó como troyano/adware, con modificación de contenidos y riesgo de exfiltración de credenciales. Las medidas aplicadas han mitigado la amenaza inmediata. Es imprescindible implementar las recomendaciones de un programa de monitoreo continuo para evitar re-infecciones y disminuir la superficie de ataque.

10. Anexos y checklist (para implementación inmediata)
    - Copia completa del sitio y DB (backup fuera del servidor) — hecho antes de cambios críticos.
    - Lista de archivos/quarantena (adjuntar lista de rutas de archivos maliciosos eliminados).
    - Registros de acceso relevantes (fechas y IPs sospechosas).
    - Cambios realizados en configuración (wp-config, .htaccess) documentados.
    - Acciones de bloqueo en Wordfence (reglas aplicadas).
    - Plan de monitoreo: escaneos programados + responsable asignado.