YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[datos de la empresa por completar]

Ref. informe: YH-DEMO-2026-04
Fecha de emisión: 19 de noviembre de 2026
PLAN DE RECUPERACIÓN

RESPUESTA A INCIDENTES Y REMEDIACIÓN • ENTREGABLE N.º 4

Análisis de incidentes y recuperación integral

Diagnóstico de un error 502 breve, investigación forense de acceso no autorizado y plan de desinfección / endurecimiento.

CLIENTE DESTINATARIO

Sociedad: Horizons Médias & Édition SARL (Ficticio)
Dominios: portail-horizons.example (+ multisitio)
Servidor host: srv-demo-03.yoorhosting.com (Nginx/Apache)
Cuentas: horizons_adm · horizons_wp

ERROR HTTP 502 EXPLICADO
12 s · 85 req
Reinicio de Apache tras actualización

VECTOR DE ENTRADA INICIAL
1 cuenta FTP
Credenciales de agencia sin chroot

PROPAGACIÓN EN SERVIDOR
0 propagación
Otras cuentas cPanel y SSH intactos

PROTOCOLO DE REMEDIACIÓN
10 etapas
Reconstrucción limpia y endurecimiento

SOLICITUD DEL CLIENTE

«Tras alertas de indisponibilidad puntual (error 502) y sospechas posteriores de accesos no autorizados y envío masivo de correo no deseado en un alojamiento multisitio, el cliente solicitó: (1) la explicación técnica exacta del corte 502, (2) la investigación forense completa de la intrusión y su alcance, y (3) un protocolo técnico detallado de recuperación limpia y endurecimiento duradero.»

1 Parte 1 — Análisis de indisponibilidad breve (Error HTTP 502 de 12 segundos)

CRONOLOGÍA DE REGISTROS (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : actualización auto openssl,
systemd, ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload y
reinicios en cola
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : corte upstream
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused durante
parada de Apache
[14:28:00-01] Apache reiniciado (OpenSSL/3.5.8) → 100
% HTTP 200 OK
```

Constatación: El 100 % de los **85 errores 502** ocurrieron en esos 12 segundos. Sin archivos corruptos, ataque externo ni fallo de hardware. Comprobaciones tras el reinicio: inicio (~180 ms), ficha producto (~210 ms) y admin (~150 ms) todos en `200 OK`.

ANOMALÍA ASOCIADA EN BACK-OFFICE Y RECOMENDACIONES

Los registros aplicativos (`/home/horizons_adm/public_html/var/logs/`) revelaron un error distinto al abrir *Información del sistema* por `operateur@portail-horizons.example` :

```
FatalError: Maximum execution time of 180 seconds
exceeded
at .../classes/ConfigurationTest.php:246 (escaneo
recursivo /img/)
```

- Programar las actualizaciones del sistema en horario nocturno (02:00–05:00).
- Priorizar la recarga sin corte (`httpd -k graceful` / `systemctl reload`) frente a paradas completas.
- Evitar el escaneo recursivo de `/img/` en horario comercial en `ConfigurationTest.php` .

2 Parte 2 — Investigación forense de acceso no autorizado

VECTOR DE ENTRADA INICIAL Y DEFECTO DE AISLAMIENTO

No se explotó ningún fallo zero-day. Tras un intento fallido en cPanel (puerto 2083) a las 08:26 UTC desde `203.0.113.10`, el atacante se autenticó al primer intento por FTP (puerto 21) a las 15:17 UTC con credenciales válidas de la cuenta de proveedor `agence-ext@portail-horizons.example`. **Defecto clave:** esta cuenta FTP apuntaba a la raíz de cPanel `/home/horizons_adm` en lugar de estar confinada (*chroot*) en `public_html`, dando acceso a los archivos de configuración y a las credenciales de MariaDB (`horizons_dbprod`).

FECHA / HORA (UTC)	IP (ANONIMIZADA)	ORIGEN / RELÉ	ACCIONES RECONSTRUIDAS (MISMA HUELLA FTP + `CURL/8.7.1`)
15/09 08:26	`203.0.113.10`	Proveedor VPS A	Intentos fallidos en cPanel (puerto 2083) con el usuario de la cuenta.
15/09 15:17	`203.0.113.10`	Proveedor VPS A	Primera conexión FTP exitosa (`agence-ext@...`); lectura de `tools/.htaccess` y script de prueba eliminado.
16/09 02:21	`203.0.113.10`	Proveedor VPS A	Subida del skimmer JavaScript `themes/universal/assets/js/custome1.js` (64 210 bytes) y alteración de `payment.tpl`.
22/09 12:29	`203.0.113.21`	Relé Proxy B	Descarga FTP de `app/config/parameters.php` (acceso MariaDB y claves); depósito de backdoor `_ca_9f3a.php`.
23/09 15:37–19:31	`203.0.113.22/23/24`	Proxys rotativos C/D/E	Subida de `clearcache.php`, extracción API de pedidos (`/api/orders` en bloques de 500) y reconocimiento de sistema (10 KB).
23/09–08/10	`203.0.113.50`	Servidor VPS F	Webshells `_npgop_*.php`, consultas SQL en Base64, controladores falsificados en pasarela de pago y script de borrado `npg_purge.json`.

ALTERACIONES APLICATIVAS Y EN BASE SQL

- **Base MariaDB (`horizons_db2025`):** activación de `PS_WEBSERVICE`, cambio de `PS_MAIL_METHOD`, reactivación de módulos de terceros, lectura de pedidos y purga selectiva de registros de auditoría.
- **Skimmer JS:** interceptaba los campos del formulario de pago y exfiltraba los datos en Base64 vía `sendBeacon` / `fetch` hacia un servidor colector externo (`collecte-tiers.example`).
- **Pasarela de pago:** inyección de controladores paralelos (`npginit.php`) y archivos ocultos de estado bajo `var/.ppext/`.

VERIFICACIÓN DE AISLAMIENTO EN SRV-DEMO-03

ALCANCE VERIFICADO	OBSERVACIÓN	ESTADO
Otras cuentas cPanel (`tiers_a`, `tiers_b`)	Ningún archivo, log ni petición sospechosa	INTACTO
Acceso SSH y sistema (`/var/log/secure*`)	Cero intentos desde las IP atacantes	INTACTO
Tareas Cron (`/etc/cron*`)	Únicamente scripts de negocio legítimos	LIMPIO
Procesos activos en memoria	Solo PHP-FPM y copias de seguridad	LIMPIO

3 Parte 3 — Auditoría multisitio y plan completo de desinfección y endurecimiento

CONSTATACIONES QUE JUSTIFICAN UNA RECONSTRUCCIÓN LIMPIA (CUENTA `HORIZONS_WP`)

- **CRÍTICO** Más de **410 000 correos spam** enviados en 30 días desde buzones secuestrados y scripts PHP directos.
- **CRÍTICO** Hasta **83 webshells** por sitio en 6 de los 7 dominios (`editions-alpha.example`, `atelier-beta.example`).
- **CRÍTICO** Cuentas de administrador WordPress ilegítimas, plugin oculto «must-use» y redirección SEO maliciosa.
- **49 buzones de correo** creados por los atacantes y conexiones desde IP desconocidas (contraseñas comprometidas).
- Plugins obsoletos con fallos conocidos (`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`).
- Falta de endurecimiento: editor de archivos activo, `XML-RPC` abierto y formularios sin captcha.

#	ETAPA DE RECUPERACIÓN	ACCIONES TÉCNICAS PREVISTAS EN EL PROTOCOLO DE REMEDIACIÓN
1	**Contención de urgencia**	Bloqueo inmediato de todo envío de spam saliente, cierre de accesos atacantes y copia probatoria completa de la cuenta comprometida.
2	**Triaje forense e inventario**	Separación de los contenidos legítimos de cada dominio frente a archivos, carpetas, usuarios y registros SQL plantados por el atacante.
3	**Nueva cuenta aislada**	Creación de una cuenta cPanel limpia, renovación total de contraseñas (panel, FTP, base de datos, correo, WordPress), SSH cerrado, un único FTP con chroot.
4	**Reconstrucción limpia**	Reinstalación del núcleo, tema y plugins desde fuentes oficiales; purga SQL de administradores falsos, enlaces inyectados y opciones maliciosas; medios sin código ejecutable.
5	**Modernización de plugins**	Actualización o sustitución de todas las extensiones obsoletas, pruebas funcionales y eliminación de módulos no utilizados.
6	**Protección de formularios**	Protección antibot (Turnstile o hCaptcha), campo honeypot, límite de tasa por IP, destinatario fijo y envío exclusivo por SMTP autenticado.
7	**Saneamiento de correo**	Conservación única de buzones confirmados, eliminación de buzones piratas, límites de envío y configuración `SPF`, `DKIM` y `DMARC`.
8	**Endurecimiento completo**	Desactivación del editor de archivos, cierre de `XML-RPC`, bloqueo de ejecución PHP en `uploads`, doble factor (2FA) en admins, reglas WAF y actualizaciones automáticas.
9	**Baja de dominios infectados**	Eliminación segura de los sitios creados por los atacantes y control DNS completo de cada dominio conservado.
10	**Seguimiento 30 días e informe**	Vigilancia continua de archivos y correo saliente, control de verificación en el día 7 y entrega de informe escrito detallando todo lo eliminado, reconstruido y endurecido.

Recomendaciones complementarias (Parte 2 y Parte 3): revocar de inmediato la clave Webservice (`API_KEY_REVOQUEE_DEMO_01`) y las cuentas FTP antiguas, eliminar `custome1.js` y `clearcache.php`, reinstalar una versión oficial del módulo de pago y notificar a la entidad bancaria adquirente y a la autoridad competente si pudieron interceptarse transacciones entre el 16/09 y el 08/10.

Validación técnica:
Unidad CERT y Seguridad Operativa — YOORshop SAS

✓ Protocolo Validado