**YOORshop SAS**
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[informations de société à compléter]

**Réf. rapport :** YH-DEMO-2026-04
**Date d'émission :** 19 novembre 2026
PLAN DE REMISE EN ÉTAT

RÉPONSE À INCIDENT & REMÉDIATION • LIVRABLE N°4

# Analyse d'incidents et remise en état

Diagnostic d'une erreur 502 brève, investigation forensique d'accès non autorisé et plan de désinfection / durcissement.

**CLIENT DESTINATAIRE**
**Société :** Horizons Médias & Édition SARL (Fictif)
**Domaines :** portail-horizons.example (+ multi-sites)
**Serveur hôte :** srv-demo-03.yoorhosting.com (Nginx/Apache)
**Comptes :** horizons_adm · horizons_wp

| ERREUR HTTP 502 EXPLIQUÉE | VECTEUR D'ENTRÉE INITIAL | PROPAGATION SERVEUR HÔTE | PROTOCOLE DE REMÉDIATION |
|---|---|---|---|
| **12 s · 85 req** | **1 compte FTP** | **0 propagation** | **10 étapes** |
| Redémarrage Apache post-mise à jour | Identifiants agence sans chroot racine | Autres comptes cPanel et SSH intacts | Reconstruction propre et durcissement |

**DEMANDE DU CLIENT**

« À la suite d'alertes d'indisponibilité ponctuelle (erreur 502), puis de suspicions d'accès non autorisés et d'envois massifs de courriels non sollicités sur un hébergement multi-sites, le client a demandé : (1) l'explication technique exacte de la coupure 502, (2) l'investigation complète de l'intrusion et de son périmètre, et (3) un protocole technique détaillé de remise en état et de durcissement durable. »

## 1 Volet 1 — Analyse d'indisponibilité brève (Erreur HTTP 502 de 12 secondes)

### CHRONOLOGIE DES JOURNAUX (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : mise à jour auto openssl,
systemd, ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload et mise en
file d'attente
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : rupture upstream
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused pendant
l'arrêt Apache
[14:28:00-01] Apache redémarré (OpenSSL/3.5.8) → 100
% HTTP 200 OK
```

**Constat :** 100 % des **85 erreurs 502** se sont produites durant ces 12 secondes. Aucun fichier corrompu, aucune attaque ni panne matérielle. Vérifications après reprise : accueil (~180 ms), fiche produit (~210 ms) et admin (~150 ms) tous en `200 OK`.

### ANOMALIE BACK-OFFICE ASSOCIÉE & PRÉCONISATIONS

Les journaux applicatifs ( `/home/horizons_adm/public_html/var/logs/` ) ont révélé une erreur distincte lors de l'ouverture de *Informations système* par `operateur@portail-horizons.example` :

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

- Planifier les mises à jour système en fenêtre nocturne (02h00–05h00).
- Privilégier un rechargement gracieux ( `httpd -k graceful` / `systemctl reload` ) plutôt qu'un arrêt/relance complet.
- Éviter le scan récursif `/img/` en journée dans `ConfigurationTest.php` .

## 2 Volet 2 — Investigation forensique d'accès non autorisé

### VECTEUR D'ENTRÉE INITIAL & DÉFAUT DE CLOISONNEMENT

Aucune faille zero-day n'a été exploitée. Après une tentative échouée sur cPanel (port 2083) à 08:26 UTC depuis `203.0.113.10`, l'attaquant s'est authentifié du premier coup en FTP (port 21) à 15:17 UTC avec les identifiants valides du compte prestataire `agence-ext@portail-horizons.example`. **Défaut clé :** ce compte FTP pointait sur la racine cPanel `/home/horizons_adm` au lieu d'être confiné (*chroot*) sur `public_html`, donnant accès aux fichiers de configuration et aux identifiants MariaDB (`horizons_dbprod`).

| DATE / HEURE (UTC) | IP (ANONYMISÉE) | ORIGINE / RELAIS | ACTIONS RECONSTITUÉES (MÊME SIGNATURE FTP + `CURL/8.7.1`) |
|---|---|---|---|
| 15/09 08:26 | `203.0.113.10` | Hébergeur VPS A | Tentatives infructueuses sur cPanel (port 2083) avec le login compte. |
| 15/09 15:17 | `203.0.113.10` | Hébergeur VPS A | Première connexion FTP réussie (`agence-ext@...`) ; lecture `tools/.htaccess` et script test supprimé. |
| 16/09 02:21 | `203.0.113.10` | Hébergeur VPS A | Dépôt du skimmer JavaScript `themes/universal/assets/js/custome1.js` (64 210 octets) et altération de `payment.tpl`. |
| 22/09 12:29 | `203.0.113.21` | Relais Proxy B | Téléchargement FTP de `app/config/parameters.php` (accès MariaDB et clés) ; dépôt backdoor `_ca_9f3a.php`. |
| 23/09 15:37–19:31 | `203.0.113.22/23/24` | Proxys rotatifs C/D/E | Dépôt de `clearcache.php`, aspiration API commandes (`/api/orders` par blocs de 500) et reconnaissance système (10 Ko). |
| 23/09–08/10 | `203.0.113.50` | Serveur VPS F | Webshells `_npgop_*.php`, requêtes SQL encodées Base64, contrôleurs falsifiés sur passerelle de paiement, puis script `npg_purge.json` d'effacement de traces. |

### ALTÉRATIONS APPLICATIVES ET BASE SQL

- **Base MariaDB (`horizons_db2025`) :** activation `PS_WEBSERVICE`, modification `PS_MAIL_METHOD`, réactivation modules tiers, lecture commandes et purge sélective des journaux d'audit.
- **Skimmer JS :** interceptait les champs du paiement et exfiltrait les données encodées Base64 via `sendBeacon` / `fetch` vers un serveur collecteur tiers (`collecte-tiers.example`).
- **Passerelle paiement :** injection de contrôleurs parallèles (`npginit.php`) et fichiers d'état sous `var/.ppext/`.

### VÉRIFICATION D'ISOLEMENT SUR SRV-DEMO-03

| PÉRIMÈTRE CONTRÔLÉ | OBSERVATION | ÉTAT |
|---|---|---|
| Autres comptes cPanel (`tiers_a`, `tiers_b`) | Aucun fichier, log ni requête suspecte | INTACT |
| Accès SSH & système (`/var/log/secure*`) | Zéro tentative depuis les IP attaquantes | INTACT |
| Tâches Cron (`/etc/cron*`) | Uniquement scripts métier légitimes | SAIN |
| Processus actifs en mémoire | Uniquement PHP-FPM & sauvegardes | SAIN |

## 3 Volet 3 — Audit multi-sites et plan complet de désinfection & durcissement

### CONSTATS JUSTIFIANT UNE RECONSTRUCTION PROPRE (COMPTE `HORIZONS_WP`)

- **CRITIQUE** Plus de **410 000 spams** envoyés en 30 jours depuis des boîtes détournées et scripts PHP directs.
- **CRITIQUE** Jusqu'à **83 webshells** par site sur 6 des 7 domaines (`editions-alpha.example`, `atelier-beta.example`).
- **CRITIQUE** Comptes administrateurs WordPress illégitimes, plugin caché « must-use » et redirection SEO pirate.
- **49 boîtes mail** créées par les attaquants et connexions depuis des IP inconnues (mots de passe compromis).
- Extensions obsolètes avec failles connues (`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`).
- Absence de durcissement : éditeur de fichiers actif, `XML-RPC` ouvert, formulaires sans captcha.

| # | ÉTAPE DE REMISE EN ÉTAT | ACTIONS TECHNIQUES PRÉVUES DANS LE PROTOCOLE DE REMÉDIATION |
|---|---|---|
| 1 | **Confinement d'urgence** | Blocage immédiat de tout envoi de spam sortant, verrouillage des accès attaquants, sauvegarde probatoire complète du compte compromis. |
| 2 | **Tri forensique & inventaire** | Séparation des contenus légitimes de chaque domaine par rapport aux fichiers, dossiers, comptes et entrées de base plantés par l'attaquant. |
| 3 | **Nouveau compte cloisonné** | Création d'un compte cPanel sain, renouvellement intégral des mots de passe (panneau, FTP, base de données, mail, WordPress), SSH fermé, un seul utilisateur FTP restreint en chroot. |
| 4 | **Reconstruction propre** | Réinstallation du cœur, du thème et des extensions depuis les sources officielles ; purge SQL des administrateurs frauduleux, liens injectés et options malveillantes ; restauration des médias sans code exécutable. |
| 5 | **Modernisation des plugins** | Mise à jour ou remplacement de toutes les extensions obsolètes, tests fonctionnels et suppression des modules inutilisés. |
| 6 | **Sécurisation des formulaires** | Protection anti-bot (Turnstile ou hCaptcha), champ pot-de-miel, limitation de débit par IP, destinataire fixe et envoi exclusif via SMTP authentifié. |
| 7 | **Assainissement e-mail** | Conservation des seules boîtes confirmées, suppression des boîtes pirates, plafonds d'envoi, configuration `SPF`, `DKIM` et `DMARC`. |
| 8 | **Durcissement complet** | Désactivation de l'éditeur de fichiers, fermeture `XML-RPC`, blocage d'exécution PHP dans `uploads`, double authentification (2FA) admins, règles WAF et mises à jour de sécurité automatiques. |
| 9 | **Décommissionnement** | Suppression sécurisée des sites créés uniquement par les attaquants et contrôle DNS complet de chaque domaine conservé. |
| 10 | **Suivi 30 jours & rapport** | Surveillance continue des fichiers et des flux mail sortants, contrôle de vérification à J+7 et remise du rapport écrit détaillant tout ce qui a été supprimé, reconstruit et durci. |

**Recommandations complémentaires (Volet 2 & Volet 3) :** révoquer immédiatement la clé Webservice (`API_KEY_REVOQUEE_DEMO_01`) et les anciens comptes FTP, supprimer `custome1.js` et `clearcache.php`, réinstaller une version officielle de la passerelle de paiement, et notifier l'acquéreur bancaire ainsi que l'autorité compétente si des transactions ont pu être interceptées entre le 16/09 et le 08/10.

**Validation technique :**
Cellule CERT & Sécurité Opérationnelle — YOORshop SAS

✓ **Protocole Validé**