**YOORshop SAS**
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[dati aziendali da completare]

**Rif. rapporto:** YH-DEMO-2026-04
**Data di emissione:** 19 novembre 2026
PIANO DI RIPRISTINO

RISPOSTA AGLI INCIDENTI E BONIFICA • LIVRABILE N. 4

# Analisi degli incidenti e ripristino completo

Diagnosi di un breve errore 502, indagine forense su accesso non autorizzato e piano di bonifica / hardening.

**CLIENTE DESTINATARIO**
**Società:** Horizons Médias & Édition SARL (Fittizio)
**Domini:** portail-horizons.example (+ multi-sito)
**Server host:** srv-demo-03.yoorhosting.com (Nginx/Apache)
**Account:** horizons_adm · horizons_wp

**ERRORE HTTP 502 CHIARITO**
**12 s · 85 req**
Riavvio Apache post-aggiornamento

**VETTORE D'INGRESSO INIZIALE**
**1 account FTP**
Credenziali agenzia senza chroot

**PROPAGAZIONE SUL SERVER**
**0 propagazione**
Altri account cPanel e SSH intatti

**PROTOCOLLO DI BONIFICA**
**10 fasi**
Ricostruzione pulita e hardening

**RICHIESTA DEL CLIENTE**

«A seguito di avvisi di indisponibilità temporanea (errore 502) e di successivi sospetti di accessi non autorizzati e invio massivo di email indesiderate su un hosting multi-sito, il cliente ha richiesto: (1) la spiegazione tecnica esatta dell'interruzione 502, (2) l'indagine forense completa sull'intrusione e sul suo perimetro e (3) un protocollo tecnico dettagliato di ripristino pulito e hardening duraturo.»

## 1 Parte 1 — Analisi della breve indisponibilità (Errore HTTP 502 di 12 secondi)

### CRONOLOGIA DEI LOG (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : aggiornamento auto openssl,
systemd, ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload e riavvii
accodati
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : interruzione upstream
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused durante
l'arresto di Apache
[14:28:00-01] Apache riavviato (OpenSSL/3.5.8) → 100
% HTTP 200 OK
```

**Riscontro:** Il 100 % degli **85 errori 502** si è verificato in quei 12 secondi. Nessun file corrotto, nessun attacco né guasto hardware. Verifiche dopo il ripristino: home (~180 ms), scheda prodotto (~210 ms) e admin (~150 ms) tutti in `200 OK`.

### ANOMALIA BACK-OFFICE ASSOCIATA E RACCOMANDAZIONI

I log applicativi ( `/home/horizons_adm/public_html/var/logs/` ) hanno evidenziato un errore distinto all'apertura di *Informazioni di sistema* da parte di `operateur@portail-horizons.example` :

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

- Pianificare gli aggiornamenti di sistema in fascia notturna (02:00–05:00).
- Preferire il ricaricamento senza interruzioni ( `httpd -k graceful` / `systemctl reload` ) rispetto ad arresto/avvio completo.
- Evitare la scansione ricorsiva di `/img/` nelle ore lavorative in `ConfigurationTest.php` .

## 2 Parte 2 — Indagine forense sull'accesso non autorizzato

### VETTORE D'INGRESSO INIZIALE E DIFETTO DI CONFINAMENTO

Non è stata sfruttata alcuna vulnerabilità zero-day. Dopo un tentativo fallito su cPanel (porta 2083) alle 08:26 UTC da `203.0.113.10`, l'attaccante si è autenticato al primo colpo via FTP (porta 21) alle 15:17 UTC con le credenziali valide dell'account fornitore `agence-ext@portail-horizons.example`. **Difetto chiave:** questo account FTP puntava alla radice cPanel `/home/horizons_adm` anziché essere confinato (*chroot*) su `public_html`, dando accesso ai file di configurazione e alle credenziali MariaDB (`horizons_dbprod`).

| DATA / ORA (UTC) | IP (ANONIMIZZATO) | ORIGINE / RELAY | AZIONI RICOSTRUITE (STESSA IMPRONTA FTP + `CURL/8.7.1`) |
|---|---|---|---|
| 15/09 08:26 | `203.0.113.10` | Provider VPS A | Tentativi falliti su cPanel (porta 2083) con il login dell'account. |
| 15/09 15:17 | `203.0.113.10` | Provider VPS A | Prima connessione FTP riuscita (`agence-ext@...`); lettura di `tools/.htaccess` e script di test rimosso. |
| 16/09 02:21 | `203.0.113.10` | Provider VPS A | Caricamento dello skimmer JavaScript `themes/universal/assets/js/custome1.js` (64 210 byte) e modifica di `payment.tpl`. |
| 22/09 12:29 | `203.0.113.21` | Relay Proxy B | Download FTP di `app/config/parameters.php` (accesso MariaDB e chiavi); deposito backdoor `_ca_9f3a.php`. |
| 23/09 15:37–19:31 | `203.0.113.22/23/24` | Proxy rotanti C/D/E | Caricamento di `clearcache.php`, estrazione API ordini (`/api/orders` a blocchi di 500) e ricognizione di sistema (10 KB). |
| 23/09–08/10 | `203.0.113.50` | Server VPS F | Webshell `_npgop_*.php`, query SQL codificate in Base64, controller falsificati sul gateway di pagamento e script `npg_purge.json` di rimozione tracce. |

### ALTERAZIONI APPLICATIVE E DATABASE SQL

- **Database MariaDB (`horizons_db2025`):** attivazione `PS_WEBSERVICE`, modifica `PS_MAIL_METHOD`, riattivazione moduli terzi, lettura ordini e pulizia selettiva dei log di audit.
- **Skimmer JS:** intercettava i campi del pagamento ed esfiltrava i dati codificati in Base64 via `sendBeacon` / `fetch` verso un server di raccolta terzo (`collecte-tiers.example`).
- **Gateway di pagamento:** iniezione di controller paralleli (`npginit.php`) e file di stato nascosti sotto `var/.ppext/`.

### VERIFICA D'ISOLAMENTO SU SRV-DEMO-03

| PERIMETRO CONTROLLATO | OSSERVAZIONE | STATO |
|---|---|---|
| Altri account cPanel (`tiers_a`, `tiers_b`) | Nessun file, log o richiesta sospetta | INTATTO |
| Accesso SSH e sistema (`/var/log/secure*`) | Zero tentativi dagli IP attaccanti | INTATTO |
| Task Cron (`/etc/cron*`) | Unicamente script applicativi legittimi | PULITO |
| Processi attivi in memoria | Solo PHP-FPM e backup regolari | PULITO |

## 3 Parte 3 — Audit multi-sito e piano completo di bonifica e hardening

### RISCONTRI CHE RICHIEDONO UNA RICOSTRUZIONE PULITA (ACCOUNT `HORIZONS_WP`)

- **CRITICO** Oltre **410 000 email di spam** inviate in 30 giorni da caselle compromesse e script PHP diretti.
- **CRITICO** Fino a **83 webshell** per sito su 6 dei 7 domini (`editions-alpha.example`, `atelier-beta.example`).
- **CRITICO** Account amministratore WordPress abusivi, plugin nascosto «must-use» ruba-password e redirect SEO malevoli.
- **49 caselle email** create dagli attaccanti e accessi da IP sconosciuti (password compromesse).
- Plugin obsoleti con vulnerabilità note (`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`).
- Assenza di hardening: editor dei file attivo, `XML-RPC` aperto, moduli di contatto privi di captcha.

| # | FASE DI RIPRISTINO | AZIONI TECNICHE PREVISTE NEL PROTOCOLLO DI BONIFICA |
|---|---|---|
| 1 | **Contenimento d'urgenza** | Blocco immediato di ogni invio spam in uscita, revoca degli accessi attaccanti, backup forense completo dell'account compromesso. |
| 2 | **Triage forense e inventario** | Separazione dei contenuti legittimi di ciascun dominio da file, cartelle, account e record SQL inseriti dall'attaccante. |
| 3 | **Nuovo account isolato** | Creazione di un account cPanel pulito, rotazione completa delle password (pannello, FTP, DB, mail, WordPress), SSH chiuso, un solo utente FTP in chroot. |
| 4 | **Ricostruzione pulita** | Reinstallazione di core, tema ed estensioni da fonti ufficiali; pulizia SQL di admin abusivi, link iniettati e opzioni malevole; ripristino media senza codice eseguibile. |
| 5 | **Modernizzazione dei plugin** | Aggiornamento o sostituzione di tutti i plugin obsoleti, test funzionali e rimozione dei moduli inutilizzati. |
| 6 | **Protezione dei moduli** | Protezione anti-bot (Turnstile o hCaptcha), campo honeypot, rate-limit per IP, destinatario fisso e invio esclusivo tramite SMTP autenticato. |
| 7 | **Bonifica email** | Mantenimento delle sole caselle confermate, eliminazione delle caselle abusive, limiti d'invio e configurazione `SPF`, `DKIM` e `DMARC`. |
| 8 | **Hardening completo** | Disattivazione dell'editor file, chiusura `XML-RPC`, blocco esecuzione PHP in `uploads`, doppia autenticazione (2FA) admin, regole WAF e aggiornamenti automatici. |
| 9 | **Dismissione domini** | Rimozione sicura dei siti creati dagli attaccanti e controllo DNS completo per ogni dominio mantenuto. |
| 10 | **Monitoraggio 30 giorni e report** | Sorveglianza continua dei file e del traffico mail in uscita, verifica al giorno 7 e consegna del rapporto scritto con tutto ciò che è stato rimosso, ricostruito e protetto. |

**Raccomandazioni complementari (Parte 2 e Parte 3):** revocare immediatamente la chiave Webservice (`API_KEY_REVOQUEE_DEMO_01`) e i vecchi account FTP, eliminare `custome1.js` e `clearcache.php`, reinstallare una versione ufficiale del modulo di pagamento e informare la banca acquirente e l'autorità competente qualora siano state intercettate transazioni tra il 16/09 e l'08/10.

**Validazione tecnica:**
Unità CERT e Sicurezza Operativa — YOORshop SAS

✓ **Protocollo Validato**