YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[company details to be completed]

Report Ref.: YH-DEMO-2026-04
Issue Date: November 19, 2026
REMEDIATION PLAN

INCIDENT RESPONSE & REMEDIATION • DELIVERABLE #4

Incident Analysis & Full Remediation

Brief 502 error root-cause analysis, unauthorized access forensic investigation, and disinfection / hardening plan.

RECIPIENT CLIENT

Company: Horizons Médias & Édition SARL (Fictional)
Domains: portail-horizons.example (+ multi-site)
Host Server: srv-demo-03.yoorhosting.com (Nginx/Apache)
Accounts: horizons_adm · horizons_wp

HTTP 502 ERROR EXPLAINED
12 s · 85 req
Post-update Apache service restart

INITIAL ENTRY VECTOR
1 FTP account
Agency credentials without root chroot

HOST SERVER SPREAD
0 spread
Other cPanel accounts and SSH intact

REMEDIATION PROTOCOL
10 steps
Clean rebuild and full hardening

CLIENT REQUEST

"Following alerts of a brief outage (HTTP 502 error), and subsequent suspicions of unauthorized access and mass unsolicited email dispatch on a multi-site hosting account, the client requested: (1) the exact technical explanation of the 502 outage, (2) a full forensic investigation of the intrusion and its scope, and (3) a detailed technical protocol for clean restoration and long-term hardening."

1 Part 1 — Brief Outage Analysis (12-Second HTTP 502 Error)

LOG TIMELINE (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : auto update openssl, systemd,
ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload and queued
restarts
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : upstream break
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused during
Apache stop
[14:28:00-01] Apache restarted (OpenSSL/3.5.8) → 100%
HTTP 200 OK
```

Finding: 100% of the **85 HTTP 502 errors** occurred within those 12 seconds. No corrupted files, no external attack, and no hardware failure. Post-recovery checks: home (~180 ms), product page (~210 ms), and admin (~150 ms) all returning `200 OK`.

RELATED BACK-OFFICE ANOMALY & RECOMMENDATIONS

Application logs (`/home/horizons_adm/public_html/var/logs/`) revealed a separate error when `operateur@portail-horizons.example` opened the *System Information* page:

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

- Schedule system package updates during night windows (02:00–05:00).
- Use graceful reloads (`httpd -k graceful` / `systemctl reload`) instead of full stop/start cycles.
- Avoid triggering recursive `/img/` scans during business hours in `ConfigurationTest.php`.

2 Part 2 — Forensic Investigation of Unauthorized Access

INITIAL ENTRY VECTOR & ISOLATION FLAW

No zero-day vulnerability was exploited. After a failed cPanel login attempt (port 2083) at 08:26 UTC from `203.0.113.10`, the attacker authenticated on the very first attempt via FTP (port 21) at 15:17 UTC using valid contractor credentials `agence-ext@portail-horizons.example`. **Key flaw:** this FTP account was rooted at the cPanel home `/home/horizons_adm` rather than confined (*chrooted*) to `public_html`, exposing configuration files and MariaDB credentials (`horizons_dbprod`).

DATE / TIME (UTC)	IP (ANONYMIZED)	ORIGIN / RELAY	RECONSTRUCTED ACTIONS (SAME FTP FINGERPRINT + `CURL/8.7.1`)
15/09 08:26	`203.0.113.10`	VPS Host A	Failed login attempts on cPanel (port 2083) using the account username.
15/09 15:17	`203.0.113.10`	VPS Host A	First successful FTP login (`agence-ext@...`); read `tools/.htaccess` and uploaded/deleted a test script.
16/09 02:21	`203.0.113.10`	VPS Host A	Uploaded JavaScript card skimmer `themes/universal/assets/js/custome1.js` (64,210 bytes) and modified `payment.tpl`.
22/09 12:29	`203.0.113.21`	Proxy Relay B	FTP download of `app/config/parameters.php` (MariaDB credentials & keys); planted backdoor `_ca_9f3a.php`.
23/09 15:37–19:31	`203.0.113.22/23/24`	Rotating Proxies C/D/E	Uploaded `clearcache.php`, scraped orders via API (`/api/orders` in batches of 500), and ran system recon (10 KB).
23/09–08/10	`203.0.113.50`	VPS Server F	Webshells `_npgop_*.php`, Base64-encoded SQL queries, forged payment gateway controllers, then trace-wiping script `npg_purge.json`.

APPLICATION & SQL DATABASE ALTERATIONS

- **MariaDB Database (`horizons_db2025`):** enabled `PS_WEBSERVICE`, altered `PS_MAIL_METHOD`, reactivated third-party modules, queried order records, and selectively deleted audit logs.
- **JS Skimmer:** hooked checkout form fields and exfiltrated Base64-encoded data via `sendBeacon` / `fetch` to a third-party drop server (`collecte-tiers.example`).
- **Payment Gateway:** injected parallel controllers (`npginit.php`) and hidden state files under `var/.ppext/`.

CONTAINMENT VERIFICATION ON SRV-DEMO-03

CHECKED SCOPE	OBSERVATION	STATUS
Other cPanel accounts (`tiers_a`, `tiers_b`)	No suspicious files, logs, or requests	INTACT
SSH & system access (`/var/log/secure*`)	Zero attempts from attacker IPs	INTACT
Cron jobs (`/etc/cron*`)	Only legitimate business scripts	CLEAN
Active memory processes	Only regular PHP-FPM & backup tasks	CLEAN

3 Part 3 — Multi-Site Audit and Comprehensive Disinfection & Hardening Plan

FINDINGS JUSTIFYING A CLEAN REBUILD (ACCOUNT `HORIZONS_WP`)

- **CRITICAL** Over **410,000 spam emails** sent in 30 days from hijacked mailboxes and direct PHP mailer scripts.
- **CRITICAL** Up to **83 webshells** per site across 6 of 7 domains (`editions-alpha.example`, `atelier-beta.example`).
- **CRITICAL** Rogue WordPress admin accounts, hidden password-stealing "must-use" plugin, and malicious SEO redirects.
- **49 mailboxes** created by attackers and control panel/webmail logins from unknown IPs (passwords compromised).
- Severely outdated plugins with known CVEs (`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`).
- Lack of hardening: file editor enabled, `XML-RPC` open, contact forms without anti-bot captcha.

#	REMEDIATION STAGE	TECHNICAL ACTIONS INCLUDED IN THE REMEDIATION PROTOCOL
1	**Emergency Containment**	Immediate halt of all outgoing spam, locking of attacker access, full forensic evidence backup of the compromised account.
2	**Forensic Triage & Inventory**	Separation of legitimate domain content from attacker-planted files, directories, user accounts, and database rows.
3	**New Isolated Account**	Provisioning of a fresh cPanel account, full password rotation (panel, FTP, DB, mail, WordPress), SSH disabled, single chrooted FTP user.
4	**Clean Rebuild**	Reinstallation of core, theme, and plugins from official sources; SQL purge of rogue admins, injected links, and malicious options; media restored stripped of executable code.
5	**Plugin Modernization**	Update or replacement of all outdated plugins, functional testing, and removal of unused extensions.
6	**Form Protection**	Anti-bot challenge (Turnstile or hCaptcha), honeypot field, per-IP rate limiting, fixed recipient, and authenticated SMTP delivery only.
7	**Email & Reputation Cleanup**	Retention of confirmed mailboxes only, deletion of rogue mailboxes, sending quotas, and strict `SPF`, `DKIM`, and `DMARC` records.
8	**Full Hardening**	File editor disabled, `XML-RPC` closed, PHP execution blocked in `uploads`, 2FA for administrators, WAF rules, and automated security updates.
9	**Domain Decommissioning**	Secure removal of attacker-only sites and full DNS verification for every retained domain.
10	**30-Day Monitoring & Report**	Continuous file and outgoing mail monitoring, Day-7 verification check, and final written report detailing everything removed, rebuilt, and hardened.

Additional Recommendations (Part 2 & Part 3): immediately revoke the Webservice key (`API_KEY_REVOQUEE_DEMO_01`) and legacy FTP accounts, delete `custome1.js` and `clearcache.php`, reinstall an official release of the payment gateway module, and notify the acquiring bank and relevant authorities if transactions may have been intercepted between Sep 16 and Oct 8.

Technical Validation:
CERT & Operational Security Unit — YOORshop SAS

✓ Validated Protocol