YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[informații despre companie de completat]

Ref. raport: YH-DEMO-2026-04
Data emiterii: 19 noiembrie 2026
PLAN DE REMEDIERE

RĂSPUNS LA INCIDENTE ȘI REMEDIERE • LIVRABIL NR. 4

Analiza incidentelor și remediere completă

Diagnosticul unei scurte erori 502, investigație criminalistică privind accesul neautorizat și plan de dezinfecție / întărire.

CLIENT DESTINATAR
Companie: Horizons Médias & Édition SARL (Fictiv)
Domenii: portail-horizons.example (+ multi-site)
Server gazdă: srv-demo-03.yoorhosting.com (Nginx/Apache)
Conturi: horizons_adm · horizons_wp

EROARE HTTP 502 EXPLICATĂ
12 s · 85 req
Repornire Apache după actualizare

VECTOR INIȚIAL DE INTRARE
1 cont FTP
Credențiale agenție fără chroot

PROPAGARE PE SERVER
0 propagare
Celelalte conturi cPanel și SSH intacte

PROTOCOL DE REMEDIERE
10 etape
Reconstrucție curată și întărire

SOLICITAREA CLIENTULUI
„În urma alertelor de indisponibilitate punctuală (eroare 502), apoi a suspiciunilor de acces neautorizat și trimitere masivă de e-mailuri nesolicitate pe o găzduire multi-site, clientul a solicitat: (1) explicația tehnică exactă a întreruperii 502, (2) investigația completă a intruziunii și a perimetrului acesteia și (3) un protocol tehnic detaliat de reconstrucție curată și întărire durabilă.”

1 Partea 1 — Analiza indisponibilității scurte (Eroare HTTP 502 de 12 secunde)

CRONOLOGIA JURNALELOR (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : actualizare auto openssl,
systemd, ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload și punere
în coadă a repornirilor
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : întrerupere upstream
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused în timpul
opririi Apache
[14:28:00-01] Apache repornit (OpenSSL/3.5.8) → 100 %
HTTP 200 OK
```

Constatare: 100 % din cele **85 de erori 502** s-au produs în aceste 12 secunde. Niciun fișier corupt, niciun atac și nicio defecțiune hardware. Verificări după reluare: pagina principală (~180 ms), fișa produs (~210 ms) și admin (~150 ms) toate în `200 OK`.

ANOMALIE BACK-OFFICE ASOCIATĂ ȘI RECOMANDĂRI

Jurnalele aplicației (`/home/horizons_adm/public_html/var/logs/`) au relevat o eroare distinctă la deschiderea paginii *Informații sistem* de către `operateur@portail-horizons.example` :

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

- Planificarea actualizărilor de sistem în fereastra nocturnă (02:00–05:00).
- Utilizarea reîncărcării grațioase (`httpd -k graceful` / `systemctl reload`) în locul opririi/repornirii complete.
- Evitarea scanării recursive a `/img/` în timpul zilei în `ConfigurationTest.php` .

2 Partea 2 — Investigație criminalistică privind accesul neautorizat

VECTORUL INIȚIAL DE INTRARE ȘI LIPSA IZOLĂRII DIRECTORULUI

Nu a fost exploatată nicio vulnerabilitate zero-day. După o încercare eșuată pe cPanel (port 2083) la 08:26 UTC de la `203.0.113.10`, atacatorul s-a autentificat din prima încercare prin FTP (port 21) la 15:17 UTC folosind credențialele valide ale contului de furnizor `agence-ext@portail-horizons.example`. **Deficiență cheie:** acest cont FTP indica spre rădăcina cPanel `/home/horizons_adm` în loc să fie izolat (*chroot*) pe `public_html`, oferind acces la fișierele de configurare și la credențialele MariaDB (`horizons_dbprod`).

DATA / ORA (UTC)	IP (ANONIMIZAT)	ORIGINE / RELEU	ACȚIUNI RECONSTITUITE (ACEEAȘI SEMNĂTURĂ FTP + `CURL/8.7.1`)
15/09 08:26	`203.0.113.10`	Furnizor VPS A	Tentative nereușite pe cPanel (port 2083) cu numele contului.
15/09 15:17	`203.0.113.10`	Furnizor VPS A	Prima conexiune FTP reușită (`agence-ext@...`); citire `tools/.htaccess` și script de test șters.
16/09 02:21	`203.0.113.10`	Furnizor VPS A	Încărcarea skimmer-ului JavaScript `themes/universal/assets/js/custome1.js` (64 210 octeți) și alterarea `payment.tpl`.
22/09 12:29	`203.0.113.21`	Releu Proxy B	Descărcare FTP a `app/config/parameters.php` (acces MariaDB și chei); depunere backdoor `_ca_9f3a.php`.
23/09 15:37–19:31	`203.0.113.22/23/24`	Proxy-uri rotative C/D/E	Încărcare `clearcache.php`, extragere API comenzi (`/api/orders` în blocuri de 500) și recunoaștere sistem (10 KB).
23/09–08/10	`203.0.113.50`	Server VPS F	Webshell-uri `_npgop_*.php`, interogări SQL în Base64, controlere falsificate pe procesatorul de plăți, apoi scriptul `npg_purge.json` de ștergere a urmelor.

ALTERĂRI ÎN APLICAȚIE ȘI BAZA DE DATE SQL

- **Baza MariaDB (`horizons_db2025`):** activare `PS_WEBSERVICE`, modificare `PS_MAIL_METHOD`, reactivare module terțe, citire comenzi și ștergere selectivă a jurnalelor de audit.
- **Skimmer JS:** intercepta câmpurile de plată și exfiltra datele codificate în Base64 prin `sendBeacon` / `fetch` către un server colector terț (`collecte-tiers.example`).
- **Procesator plăți:** injectare de controlere paralele (`npginit.php`) și fișiere de stare ascunse în `var/.ppext/`.

VERIFICAREA IZOLĂRII PE SRV-DEMO-03

PERIMETRU CONTROLAT	OBSERVAȚIE	STARE
Alte conturi cPanel (`tiers_a`, `tiers_b`)	Niciun fișier, jurnal sau cerere suspectă	INTACT
Acces SSH și sistem (`/var/log/secure*`)	Zero tentative de la IP-urile atacatoare	INTACT
Sarcini Cron (`/etc/cron*`)	Exclusiv scripturi legitime de business	CURAT
Procese active în memorie	Doar PHP-FPM și procese de backup	CURAT

3 Partea 3 — Audit multi-site și plan complet de dezinfecție și întărire

CONSTATĂRI CARE JUSTIFICĂ O RECONSTRUCȚIE CURATĂ (CONTUL `HORIZONS_WP`)

- **CRITIC** Peste **410 000 de e-mailuri spam** trimise în 30 de zile din căsuțe deturnate și scripturi PHP directe.
- **CRITIC** Până la **83 de webshell-uri** per site pe 6 din cele 7 domenii (`editions-alpha.example`, `atelier-beta.example`).
- **CRITIC** Conturi de administrator WordPress nelegitime, plugin ascuns „must-use” și redirecționări SEO pirat.
- **49 de căsuțe e-mail** create de atacatori și conectări de la IP-uri necunoscute (parole compromise).
- Extensii învechite cu vulnerabilități cunoscute (`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`).
- Lipsă de întărire: editor de fișiere activ, `XML-RPC` deschis, formulare fără captcha.

#	ETAPĂ DE REMEDIERE	ACȚIUNI TEHNICE PREVĂZUTE ÎN PROTOCOLUL DE REMEDIERE
1	**Izolare de urgență**	Blocarea imediată a oricărei trimiteri de spam, blocarea accesului atacatorilor, backup probatoriu complet al contului compromis.
2	**Triaj criminalistic și inventar**	Separarea conținutului legitim al fiecărui domeniu față de fișierele, directoarele, conturile și înregistrările SQL plantate de atacator.
3	**Cont nou izolat**	Crearea unui cont cPanel curat, reînnoirea integrală a parolelor (panou, FTP, bază de date, mail, WordPress), SSH închis, un singur FTP restricționat în chroot.
4	**Reconstrucție curată**	Reinstalarea nucleului, temei și extensiilor din surse oficiale; curățarea SQL de administratori frauduloși, linkuri injectate și opțiuni malițioase; restaurarea fișierelor media fără cod executabil.
5	**Modernizarea pluginurilor**	Actualizarea sau înlocuirea tuturor extensiilor învechite, teste funcționale și eliminarea modulelor neutilizate.
6	**Securizarea formularelor**	Protecție anti-bot (Turnstile sau hCaptcha), câmp honeypot, limitare de debit pe IP, destinatar fix și trimitere exclusivă prin SMTP autentificat.
7	**Curățarea e-mailului**	Păstrarea doar a căsuțelor confirmate, ștergerea căsuțelor pirat, plafoane de trimitere, configurare `SPF`, `DKIM` și `DMARC`.
8	**Întărire completă**	Dezactivarea editorului de fișiere, închiderea `XML-RPC`, blocarea execuției PHP în `uploads`, autentificare în doi pași (2FA) pt. admini, reguli WAF și actualizări automate.
9	**Dezafectare domenii**	Eliminarea securizată a site-urilor create de atacatori și control DNS complet pentru fiecare domeniu păstrat.
10	**Monitorizare 30 zile și raport**	Supravegherea continuă a fișierelor și a fluxurilor mail, control de verificare în ziua 7 și predarea raportului scris detaliind tot ce a fost eliminat, reconstruit și întărit.

Recomandări complementare (Partea 2 și Partea 3): revocarea imediată a cheii Webservice (`API_KEY_REVOQUEE_DEMO_01`) și a vechilor conturi FTP, ștergerea `custome1.js` și `clearcache.php`, reinstalarea unei versiuni oficiale a procesatorului de plăți și notificarea băncii acceptatoare și a autorității competente dacă au putut fi interceptate tranzacții între 16/09 și 08/10.

Validare tehnică:
Celula CERT și Securitate Operațională — YOORshop SAS

✓ Protocol Validat