YOORshop SAS
RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com
[dane firmy do uzupełnienia]

Ref. raportu: YH-DEMO-2026-04
Data wydania: 19 listopada 2026
PLAN NAPRAWCZY

REAGOWANIE NA INCYDENTY I NAPRAWA • REZULTAT NR 4

Analiza incydentów i przywrócenie sprawności

Diagnoza krótkiego błędu 502, śledztwo kryminalistyczne po nieautoryzowanym dostępie oraz plan oczyszczenia i utwardzenia.

KLIENT DOCELOWY
Firma: Horizons Médias & Édition SARL (Fikcyjna)
Domeny: portail-horizons.example (+ multisite)
Serwer hosta: srv-demo-03.yoorhosting.com (Nginx/Apache)
Konta: horizons_adm · horizons_wp

WYJAŚNIONY BŁĄD HTTP 502
12 s · 85 żądań
Restart Apache po aktualizacji

POCZĄTKOWY WEKTOR WEJŚCIA
1 konto FTP
Dane agencji bez blokady chroot

PROPAGACJA NA SERWERZE
0 propagacji
Inne konta cPanel i SSH nienaruszone

PROTOKÓŁ NAPRAWCZY
10 etapów
Czysta odbudowa i utwardzenie

ZGŁOSZENIE KLIENTA

„Po alertach o chwilowej niedostępności (błąd 502), a następnie podejrzeniach nieautoryzowanego dostępu i masowej wysyłki spamu z hostingu wielodomenowego, klient zlecił: (1) dokładne wyjaśnienie techniczne przerwy 502, (2) pełne śledztwo kryminalistyczne dotyczące włamania i jego zasięgu oraz (3) szczegółowy protokół techniczny czystej odbudowy i trwałego zabezpieczenia.”

1 Część 1 — Analiza krótkiej niedostępności (12-sekundowy błąd HTTP 502)

CHRONOLOGIA LOGÓW (NGINX / SYSTEMD / DNF)

```
[14:25:27 CEST] dnf : auto-aktualizacja openssl,
systemd, ea-apache24-config-runtime
[14:27:43 CEST] systemd[1] : daemon-reload i
kolejkowanie restartów
[14:27:48 CEST] systemd[1] : Stopping Apache web
server...
[14:27:48] Nginx : zerwanie upstream
(https://192.0.2.10:4430/...)
[14:27:58] Nginx : 111 Connection refused podczas
zatrzymania Apache
[14:28:00-01] Apache uruchomiony (OpenSSL/3.5.8) →
100 % HTTP 200 OK
```

Ustalenie: 100 % z **85 błędów 502** wystąpiło w ciągu tych 12 sekund. Brak uszkodzonych plików, ataku czy awarii sprzętu. Testy po powrocie: strona główna (~180 ms), produkt (~210 ms) i admin (~150 ms) zwracają `200 OK`.

ODRĘBNY BŁĄD W BACK-OFFICE I ZALECENIA

Logi aplikacji (`/home/horizons_adm/public_html/var/logs/`) wykazały osobny błąd przy otwarciu *Informacji o systemie* przez `operateur@portail-horizons.example` :

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

- Planować aktualizacje systemowe w oknie nocnym (02:00–05:00).
- Stosować przeładowanie bezprzerwowe (`httpd -k graceful` / `systemctl reload`) zamiast pełnego stop/start.
- Unikać rekurencyjnego skanu `/img/` w ciągu dnia w `ConfigurationTest.php` .

2 Część 2 — Śledztwo kryminalistyczne w sprawie nieautoryzowanego dostępu

POCZĄTKOWY WEKTOR WEJŚCIA I BŁĄD IZOLACJI KATALOGÓW

Nie wykorzystano luki zero-day. Po nieudanej próbie logowania do cPanel (port 2083) o 08:26 UTC z `203.0.113.10`, atakujący zalogował się za pierwszym razem przez FTP (port 21) o 15:17 UTC poprawnymi danymi konta podwykonawcy `agence-ext@portail-horizons.example`. **Kluczowy błąd:** konto FTP wskazywało na katalog główny cPanel `/home/horizons_adm` zamiast być zamknięte (*chroot*) w `public_html`, co dało dostęp do plików konfiguracyjnych i haseł MariaDB (`horizons_dbprod`).

DATA / CZAS (UTC)	IP (ZANONIMIZOWANE)	ŹRÓDŁO / PRZEKAŹNIK	ODTWORZONE DZIAŁANIA (TA SAMA SYGNATURA FTP + `CURL/8.7.1`)
15/09 08:26	`203.0.113.10`	Hosting VPS A	Nieudane próby logowania do cPanel (port 2083) na login konta.
15/09 15:17	`203.0.113.10`	Hosting VPS A	Pierwsze udane logowanie FTP (`agence-ext@...`); odczyt `tools/.htaccess` i usunięty skrypt testowy.
16/09 02:21	`203.0.113.10`	Hosting VPS A	Wgranie skimmera JS `themes/universal/assets/js/custome1.js` (64 210 bajtów) i modyfikacja `payment.tpl`.
22/09 12:29	`203.0.113.21`	Przekaźnik Proxy B	Pobranie przez FTP `app/config/parameters.php` (dostęp MariaDB i klucze); wgranie backdoora `_ca_9f3a.php`.
23/09 15:37–19:31	`203.0.113.22/23/24`	Rotacyjne Proxy C/D/E	Wgranie `clearcache.php`, pobranie zamówień przez API (`/api/orders` w paczkach po 500) i rekonesans systemu (10 KB).
23/09–08/10	`203.0.113.50`	Serwer VPS F	Webshelle `_npgop_*.php`, zapytania SQL w Base64, fałszywe kontrolery płatności, a następnie skrypt czyszczący `npg_purge.json`.

MODYFIKACJE APLIKACJI I BAZY SQL

- **Baza MariaDB (`horizons_db2025`):** włączenie `PS_WEBSERVICE`, zmiana `PS_MAIL_METHOD`, aktywacja modułów zewnętrznych, odczyt zamówień i selektywne czyszczenie logów audytu.
- **Skimmer JS:** przechwytywał pola płatności i wysyłał dane w Base64 przez `sendBeacon` / `fetch` na zewnętrzny serwer zbierający (`collecte-tiers.example`).
- **Bramka płatności:** wstrzyknięcie równoległych kontrolerów (`npginit.php`) i plików stanu w `var/.ppext/`.

WERYFIKACJA IZOLACJI NA SRV-DEMO-03

KONTROLOWANY OBSZAR	OBSERWACJA	STAN
Inne konta cPanel (`tiers_a`, `tiers_b`)	Brak podejrzanych plików, logów i żądań	NIENARUSZONE
Dostęp SSH i system (`/var/log/secure*`)	Zero prób z adresów IP atakujących	NIENARUSZONE
Zadania Cron (`/etc/cron*`)	Wyłącznie legalne skrypty biznesowe	CZYSTE
Aktywne procesy w pamięci	Tylko PHP-FPM i kopie zapasowe	CZYSTE

3 Część 3 — Audyt wielodomenowy oraz pełny plan dezynfekcji i utwardzenia

USTALENIA UZASADNIAJĄCE CZYSTĄ ODBUDOWĘ (KONTO `HORIZONS_WP`)

- **KRYTYCZNY** Ponad **410 000 wiadomości spam** wysłanych w 30 dni z przejętych skrzynek i bezpośrednich skryptów PHP.
- **KRYTYCZNY** Do **83 webshelli** na stronę w 6 z 7 domen (`editions-alpha.example`, `atelier-beta.example`).
- **KRYTYCZNY** Fałszywe konta admina WordPress, ukryta wtyczka „must-use" kradnąca hasła i złośliwe przekierowania SEO.
- **49 skrzynek e-mail** utworzonych przez atakujących i logowania z nieznanych IP (wszystkie hasła przejęte).
- Przestarzałe wtyczki ze znanymi lukami (`WPForms 1.7.0`, `Elementor 2.4.7`, `Yoast SEO 5.7.1`).
- Brak utwardzenia: aktywny edytor plików, otwarty `XML-RPC`, formularze bez zabezpieczeń captcha.

#	ETAP NAPRAWY	DZIAŁANIA TECHNICZNE OBJĘTE PROTOKOŁEM NAPRAWCZYM
1	**Izolacja awaryjna**	Natychmiastowa blokada wychodzącego spamu, odcięcie dostępu atakujących, pełna kopia dowodowa przejętego konta.
2	**Triaż kryminalistyczny**	Oddzielenie legalnej zawartości każdej domeny od plików, katalogów, kont i wpisów bazy dodanych przez intruza.
3	**Nowe izolowane konto**	Utworzenie czystego konta cPanel, zmiana wszystkich haseł (panel, FTP, baza, poczta, WordPress), zamknięte SSH, jeden FTP w chroot.
4	**Czysta odbudowa**	Reinstalacja rdzenia, motywu i wtyczek z oficjalnych źródeł; oczyszczenie SQL z fałszywych adminów i linków; przywrócenie mediów bez kodu wykonywalnego.
5	**Modernizacja wtyczek**	Aktualizacja lub wymiana przestarzałych rozszerzeń, testy funkcjonalne i usunięcie nieużywanych modułów.
6	**Zabezpieczenie formularzy**	Ochrona antybotowa (Turnstile lub hCaptcha), pole honeypot, limity na IP, stały odbiorca i wysyłka wyłącznie przez uwierzytelniony SMTP.
7	**Oczyszczenie poczty**	Zachowanie tylko potwierdzonych skrzynek, usunięcie skrzynek intruza, limity wysyłki oraz konfiguracja `SPF`, `DKIM` i `DMARC`.
8	**Pełne utwardzenie**	Wyłączenie edytora plików, zamknięcie `XML-RPC`, blokada PHP w `uploads`, 2FA dla administratorów, reguły WAF i automatyczne łatki.
9	**Wygaszenie obcych domen**	Bezpieczne usunięcie witryn założonych przez atakujących i pełna kontrola DNS każdej zachowanej domeny.
10	**Monitoring 30 dni i raport**	Ciągły nadzór nad plikami i pocztą wychodzącą, kontrola w 7. dniu oraz pisemny raport końcowy z wykazem usuniętych, odbudowanych i zabezpieczonych elementów.

Zalecenia uzupełniające (Część 2 i Część 3): natychmiast unieważnić klucz Webservice (`API_KEY_REVOQUEE_DEMO_01`) i stare konta FTP, usunąć `custome1.js` oraz `clearcache.php`, przeinstalować oficjalny moduł płatności oraz powiadomić agenta rozliczeniowego i właściwy organ, jeśli między 16.09 a 08.10 mogło dojść do przechwycenia transakcji.

Zatwierdzenie techniczne:
Jednostka CERT i Bezpieczeństwa Operacyjnego — YOORshop SAS

✓ Protokół Zatwierdzony