

Independent magazine & online store

WordPress + WooCommerce · real incident, client details anonymised

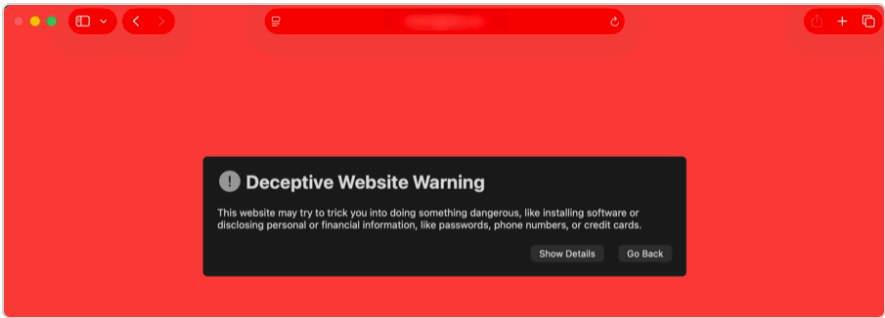
EXECUTIVE SUMMARY

An attacker logged in with a stolen admin password and spent about six weeks building hidden ways back in: disguised plugins, backdoor admin accounts and a fake “security check” popup that got the site flagged as deceptive in browsers. The site has been cleaned, every way back in we found has been closed, and it is now hardened and checked automatically every day. Card numbers were never at risk; the payment provider holds those.

INCIDENT AT A GLANCE

ENTRY POINT	Stolen admin password, captured by a fake “analytics” plugin and sent to an outside server
EXPOSURE WINDOW	About six weeks before discovery
HOW IT SURFACED	A customer reported a red “Deceptive Website Warning” in their browser
SCOPE	The WordPress site, plus two backdoor files that could run commands on the web server
DATA AT RISK	Customer names, addresses and order history readable by the attacker. No card numbers stored on the site.
STATUS	Clean, hardened and monitored daily

WHAT CUSTOMERS SAW



Browser warning caused by the injected popup · domain blurred

TIMELINE

WHEN	WHAT HAPPENED
Week 0	Earliest sign of compromise: a hidden script added to the theme that reinstalls itself if removed.
Weeks 2–5	Two hidden admin accounts created; disguised plugins installed, including one capturing every admin login.
Day 1	Customer reports the browser warning. Same-day investigation: domain not hijacked, warning traced to the injected popup. Malicious plugins, accounts and scripts removed; security keys rotated.
Day 2	Follow-up sweep finds a second, better-disguised wave: two fake themes giving command access, and the login-stealing plugin.
Days 2–6	Clean copy rebuilt on new, isolated hosting and tested. Site submitted to the browser vendor for re-review.
Day 12	Deeper server log review finds two backdoor files the first sweep missed, in a folder the site doesn't use. Removed the same day; attacker blocked; all passwords and keys changed.
Day 14	Hardening finished. Full re-scan clean. Daily automatic check switched on.

WHAT WE FOUND

FINDING	DETAIL	SEVERITY
Login-stealing plugin	Posed as an analytics add-on; sent every admin login to the attacker	CRITICAL
Hidden admin accounts x2	Hidden from the user list by another malicious plugin	CRITICAL
Fake themes x2	Copies of a default theme that let the attacker run commands	CRITICAL
Server backdoors x2	Missed by the first sweep; used every six hours until removed	CRITICAL
Fake popup x49	In the theme and six published posts; caused the browser warning	HIGH
Rogue scheduled tasks x13	Re-triggered parts of the infection after removal	HIGH
Public backups	1.1 GB full-site backup and a plugins archive anyone could download	HIGH
Paid download	Digital issue downloadable without buying it	MEDIUM
Store email	Order and password emails had silently failed for over a year	MEDIUM

HOW WE CLOSED THE WAY IN

- ✓ Every server, database and admin password changed; WordPress security keys rotated
- ✓ Plugin and theme uploads and the code editor disabled in the dashboard
- ✓ Code blocked from running in upload folders
- ✓ Eight unused plugins removed, including a file manager with a history of security holes
- ✓ Public backups deleted; paid downloads moved out of the public web folder
- ✓ Password-guessing route closed; attacker’s address blocked
- ✓ Store email restored, so order and password emails reach customers again
- ✓ Daily automatic integrity check that alerts us the morning after any unexpected change

WHERE THINGS STAND

0

infected files, hidden accounts or rogue tasks on the final re-scan

144,235

login attempts blocked by the site’s security add-on

~300

new automated attempts a day, all refused

WHAT WE NEED FROM YOU

- 1

Rotate your payment provider API keys together. The attacker could read them. A 15-minute call: we drive, you approve the two-factor prompts.

THIS WEEK
- 2

Decide whether to notify customers. Names, addresses and order history were readable. We can draft the notice.

YOUR CALL
- 3

Add a second owner to payment accounts. Right now the business depends on one phone for every security code.

SOON