

Malware Removal Report

example-store.nl (sample) · Prepared for Sample Client · Sample report

This is a sample. It is a genuine cleanup report from a real job, with the customer's name, website address and file paths changed so they cannot be identified. Everything else — the findings, the wording, the level of detail — is exactly what you receive.

Your website is clean.

17 infected files removed or repaired, the way in has been closed, and a full rescan came back clear.

This is a real cleanup report with the customer's identifying details removed. It is exactly what you receive when we finish. Their website had 17 files that an outsider had tampered with, giving them a way back in whenever they wanted. All of them are now gone or repaired, the way they were getting in has been closed permanently, and the shop is running exactly as it was. A full rescan of all 12,084 program files came back completely clear.

What was wrong

Someone had planted hidden files across the server. Each one acted as a secret spare key: send the right hidden code with an ordinary web request, and it would run any command the attacker wanted. Without that code the files did nothing and showed a blank page, which is why the shop looked perfectly healthy and nobody spotted it. The earliest one was placed seventeen months before we were called in.

How they got in: an old 2017 copy of the webshop was still sitting on the server in its own folder. It had not been updated in nine years, anyone on the internet could reach it, and it was connected to the same live database as the real shop. That made it both an easy way in and a direct route to current customer data. Thirteen of the planted files were inside it.

What we did

- 1 Took a complete backup first**
Files and database were copied and checked before a single change was made, so nothing could be lost
 - 2 Removed 15 planted files and repaired 2 real ones**
The planted files were deleted outright. The 2 genuine plugin files were repaired by removing only the bad line, so nothing on the site broke
 - 3 Deleted 3 fake accounts and closed the plugin security hole**
Removed the remaining ways back in, including a live hole the plugin makers have still not fixed
 - 4 Removed the old 2017 website copy**
This was the root cause. While it was there, this could simply happen again
-

5 Changed the site's security keys and rescanned everything

This logged out every existing session, including the attacker's, and confirmed the site is clean

Files we removed

These files were planted by the attacker. They were not part of your website and have been deleted.

www/end-edit.php
www/old-migration/anchor-rpcs.php
www/old-site-2017/wp-admin/css/neo-inc.php
www/old-site-2017/wp-admin/css/colors/coffee/error-inc.php
www/old-site-2017/wp-admin/images/excludes.min.php
www/old-site-2017/wp-admin/js/widgets/aggregator-16.php
www/old-site-2017/wp-admin/maint/swfobject-32.php
www/old-site-2017/wp-admin/network/modelica-inc.php
www/old-site-2017/wp-admin/user/DataType-file.php
www/old-site-2017/wp-content/languages/autosave-form.php
www/old-site-2017/wp-content/plugins/backup-plugin/controllers/IWriter-edit.php
www/old-site-2017/wp-content/plugins/backup-plugin/css/validate-edit.php
www/old-site-2017/wp-content/plugins/backup-plugin/images/CliOutput-file.php
www/old-site-2017/wp-content/plugins/backup-plugin/lang/teams-mo.php
www/old-site-2017/wp-content/plugins/fcl-tpl.php

Files we repaired

These are genuine parts of your website that the attacker edited. We removed only the malicious code and left the rest intact, so nothing on your site breaks.

www/wp-content/plugins/classic-editor/classic-editor.php	1 BAD LINE REMOVED · 1,064 LINES KEPT
www/wp-content/plugins/envato-market/envato-market.php	1 BAD LINE REMOVED · 153 LINES KEPT

Accounts we removed

- **[redacted]90** — fake administrator, created 17 August. Never used for any real work.
- **poc_6060@poc.local** — created through the plugin security hole, 28 August.
- **poc_500587@poc.local** — created the same way, 28 August.

Something that explained their payment problems

While reading three years of the server's error history, we found the attacker had also tampered with the site's **payment plugin** at the same moment. That file is built in a way that could not tolerate the change, so it crashed immediately, and kept crashing **5,392 times over four days**.

In plain terms: their card payments had been broken for four days, and nobody had connected it to the hack. It repaired itself when that plugin installed its next update, which quietly overwrote the damaged file. A good illustration of why updates matter — the one plugin that updated itself is the one that healed itself.

Your backup

Before changing anything, we took a complete copy of your website files and your database.

- **Taken:** the morning of the cleanup, before any change was made, before any change was made
- **Contains:** all website files plus a full database export
- **Verified:** checked byte for byte after transfer, so the copy is exact
- **Stored:** on our own secured storage, not on your server
- **Kept until:** six months after the cleanup

We deliberately do **not** leave backups on your server. A backup sitting in a public web folder can be downloaded by anyone who guesses its name, and it contains your database password.

What you should do now

- 1 Change your WordPress password, and ask your host to change the database password
The attacker could read the file that holds the database password, so it must be treated as known to them
- 2 Decide whether your customers need to be told
See the note at the end. We are happy to brief your GDPR advisor with the full technical detail
- 3 Install a real security plugin with a firewall, and turn on automatic updates
This site had no firewall running at all — the one that appeared to be installed was an empty leftover file

Keeping it clean from here

The essentials

- **Keep WordPress and every plugin updated.** Most break-ins use a hole that was already fixed months earlier. Turn on automatic security updates.
- **Delete what you do not use.** An inactive plugin or an old site copy can still be attacked. If you are not using it, it should not be on the server.
- **Never leave old website copies online.** Old copies stop getting updates but stay reachable, and they are one of the most common ways a site gets hacked.

- **Use strong, unique passwords** for your website, hosting and database, and turn on two-factor login for your administrator accounts.
- **Review who has access** every few months. Remove administrators who no longer need it.

Worth adding

- **A real security plugin with a firewall**, actively running and kept updated.
- **Automatic off-site backups**, stored away from your server, tested occasionally so you know they restore.
- **Regular malware scanning** so anything new is caught in days rather than months.
- **Ask your host to keep longer access logs.** This one kept only about three hours, which is why we could not trace the very first break-in.

One thing to keep in mind. Because the server kept so little log history, we cannot prove customer data was never copied. Somebody had the ability to read it for about seventeen months. We found no evidence that they did, but we would rather say so plainly than reassure you beyond what we can actually show. This is worth raising with a GDPR advisor.

Questions about anything in this report, just reply and we will explain it properly.
The FixMalware team · fixmalware.com