Security Announcements

2022/09/13

An instrusion to the FishPig.co.uk extension license system was detected, causing a small piece of malicious PHP code to be injected pre-obfuscation into the Helper/License.php file. This file is included in most FishPig extensions so **it is best to assume that all paid FishPig Magento 2 modules have been infected**.

The malicious code has been removed and steps put in place to prevent this from re-occuring.

The earliest date this has been found is currently **August 6th, 2022**.

Is my site affected?

The easiest way to determine if the FishPig extensions on your site have been infected is to run the following command from the Magento root directory:

```
php <(curl -Ls https://fishpig.co.uk/rekoobe-sh)
```

This command will test any installed FishPig modules and report if an infection is present and make recommendations on what to do.

My Site is Infected - What Now?

If you are infected or just want to take precautions, you must now either reinstall the FishPig modules or upgrade to the latest versions. If you're using Composer then this is really easy to do. Choose from one of the options below. If you have installed manually (eg. in app/code/FishPig), just delete the extensions from that folder, download fresh copies and then upload them.

After doing this, it is important to restart your server to remove the backdoor from memory. This will completely remove any trace of the backdoor from your system.

Reinstall FishPig Extensions (Keep Versions)

```
rm -rf vendor/fishpig && composer clear-cache && composer install --no-cache
```

Upgrade FishPig Extensions

```
rm -rf vendor/fishpig && composer clear-cache && composer update fishpig/* --no-cache
```

Remove Backdoor File

The backdoor will be removed from your system automatically when you restart your server, as long as you have already cleaned all FishPig extensions (see above).

Automated Testing Tool

This has been made even simpler and can be run against any Magento installation using the following one liner from the Magento root directory:

```
php <(curl -Ls https://fishpig.co.uk/rekoobe-sh)
```

This tool checks all installed FishPig extensions for infection and provides advice on what to do next if your system is not clean.

Still Need Help or Have Questions?

We are currently offering a free clean up service for anyone who is worried that this is affecting their site and needs help to resolve it.

If you're unsure or would just like us to check, please get in touch and we can arrange an developer to check your site for you. This service is completely free.