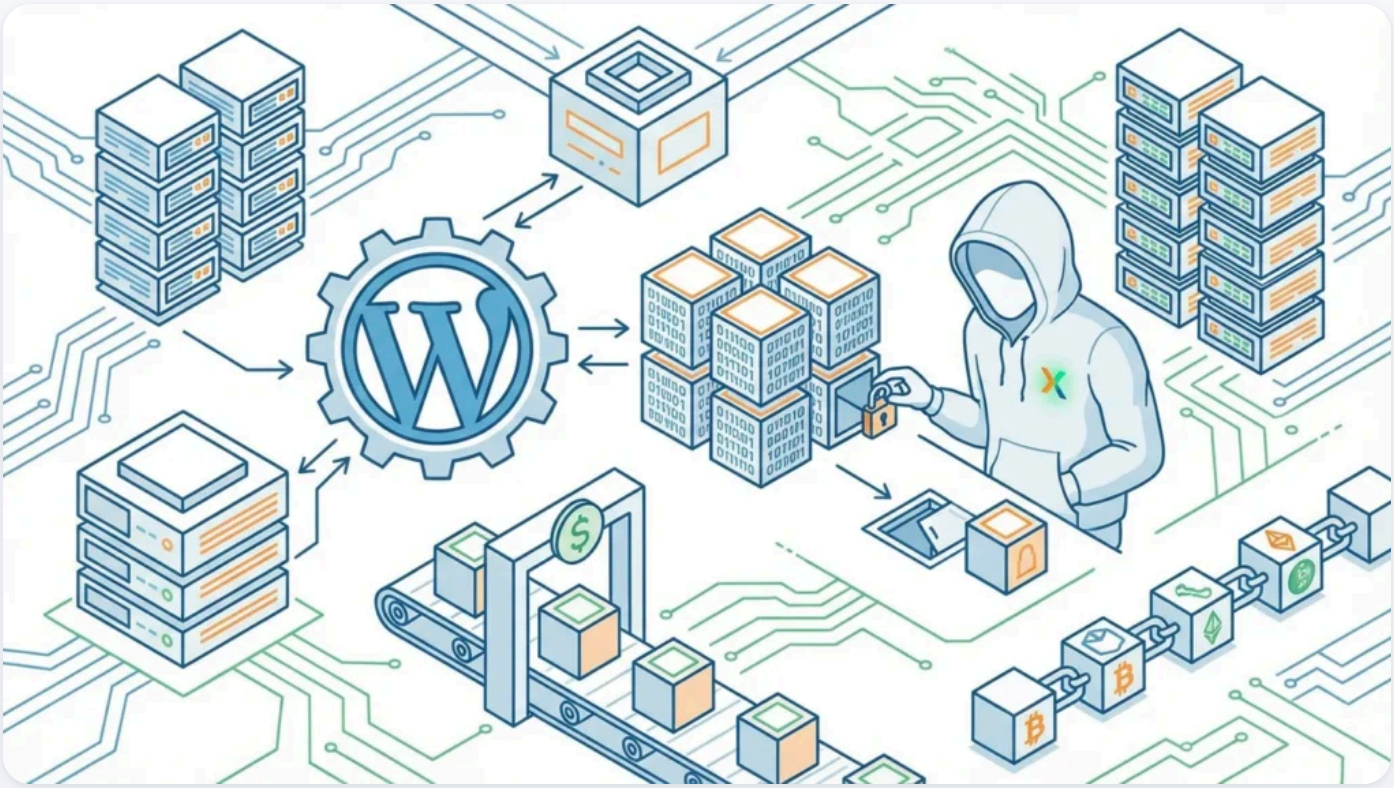
Someone Bought 30 WordPress Plugins and Planted a Backdoor in All of Them.

April 9, 2026 · Austin Ginder



Last week, I wrote about catching a supply chain attack on a WordPress plugin called Widget Logic. A trusted name, acquired by a new owner, turned into something malicious. It happened again. This time at a much larger scale.

30+
Plugins compromised

31
Closed by WordPress.org

8 months
Backdoor dormant before activation

6 figures
Paid on Flippa for the portfolio

A client reported a security notice they found in wp-admin.

Ricky from Improve & Grow emailed us about an alert he saw in the WordPress dashboard for a client site. The notice was from the WordPress.org Plugins Team, warning that a plugin called Countdown Timer Ultimate contained code that could allow unauthorized third-party access.

I ran a full security audit on the site. The plugin itself had already been force-updated by WordPress.org to version 2.6.9.1, which was supposed to clean things up. But the damage was already done.

The malware was hiding in wp-config.php.

The plugin's `wpos-analytics` module had phoned home to `analytics.essentialplugin.com`, downloaded a backdoor file called `wp-comments-posts.php` (designed to look like the core file `wp-comments-post.php`), and used it to inject a massive block of PHP into wp-config.php.

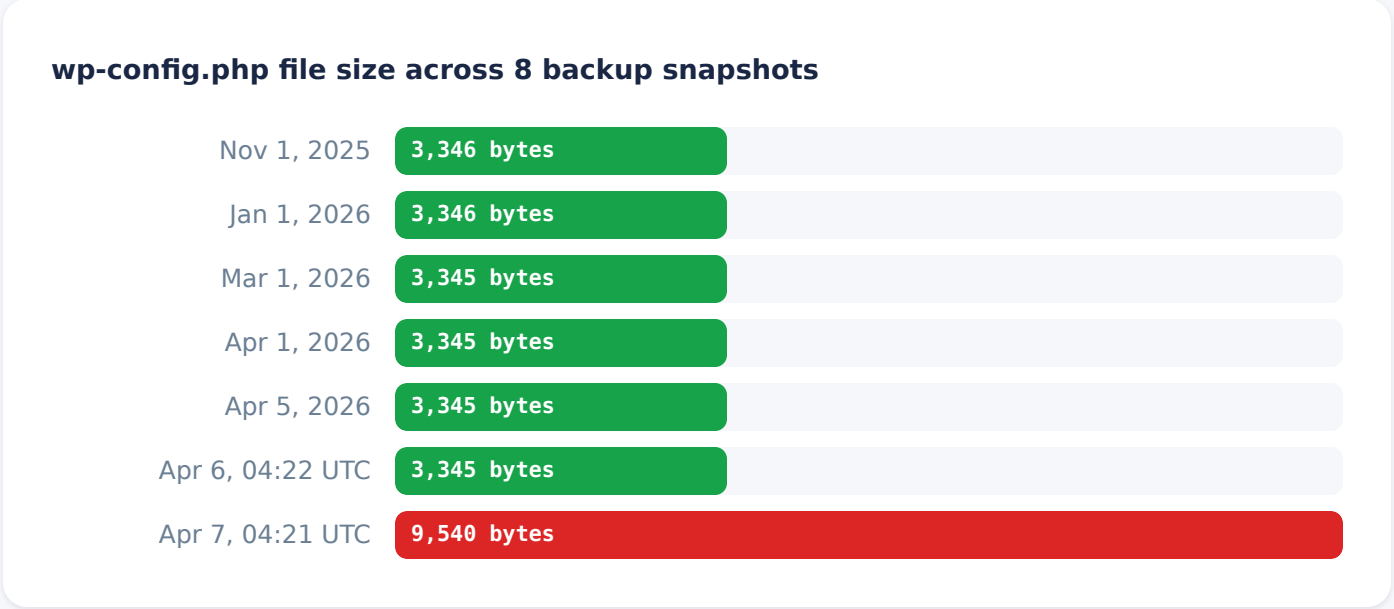
The injected code was sophisticated. It fetched spam links, redirects, and fake pages from a command-and-control server. It only showed the spam to Googlebot, making it invisible to site owners. And here is the wildest part. It resolved its C2 domain through an Ethereum smart contract, querying public blockchain RPC endpoints. Traditional domain takedowns would not work because the attacker could update the smart contract to point to a new domain at any time.

The forced update did not clean wp-config.php

WordPress.org's v2.6.9.1 update neutralized the phone-home mechanism in the plugin. But it did not touch wp-config.php. The SEO spam injection was still actively serving hidden content to Googlebot.

I used backup forensics to pinpoint the exact injection window.

CaptainCore keeps daily restic backups. I extracted wp-config.php from 8 different backup dates and compared file sizes. Binary search style.



The injection happened on April 6, 2026, between 04:22 and 11:06 UTC. A 6-hour 44-minute window.

The backdoor was planted 8 months before it was activated.

I traced the plugin's history through 939 quicksave snapshots. The plugin had been on the site since January 2019. The `wpos-analytics` module was always there, functioning as a legitimate analytics opt-in system for years.

Then came version 2.6.7, released August 8, 2025. The changelog said, "Check compatibility with WordPress version 6.8.2." What it actually did was add 191

lines of code, including a PHP deserialization backdoor. The `class-anylc-admin.php` file grew from 473 to 664 lines.

The new code introduced three things:

1. A `fetch_ver_info()` method that calls `file_get_contents()` on the attacker's server and passes the response to `@unserialize()`
2. A `version_info_clean()` method that executes `@$clean($this->version_cache, $this->changelog)` where all three values come from the unserialized remote data
3. An unauthenticated REST API endpoint with `permission_callback: __return_true`

That is a textbook arbitrary function call. The remote server controls the function name, the arguments, everything. It sat dormant for 8 months before being activated on April 5-6, 2026.

The plugin was sold on Flippa.

This is where it gets interesting. The original plugin was built by Minesh Shah, Anoop Ranawat, and Pratik Jain. An India-based team that operated under "WP Online Support" starting around 2015. They later rebranded to "Essential Plugin" and grew the portfolio to 30+ free plugins with premium versions.

By late 2024, revenue had declined 35-45%. Minesh listed the entire business on Flippa. A buyer identified only as "Kris," with a background in SEO, crypto, and online gambling marketing, purchased everything for six figures. Flippa even published a case study about the sale in July 2025.

- February 2015
  wponlinesupport.com domain registered. Team begins building WordPress plugins.
- October 2016
  Countdown Timer Ultimate published on WordPress.org by anoopranawat.
- August 2021

essentialplugin.com domain registered. Company rebrands from WP Online Support to Essential Plugin.

Late 2024

Revenue declines 35-45%. Minesh Shah lists the entire business on Flippa.

Early 2025

Buyer ‘Kris’ acquires Essential Plugin for six figures via Flippa.

May 12, 2025

New essentialplugin WordPress.org account created.

May 14-16, 2025

Last commits by the original wponlinesupport account. Author headers changed.

August 8, 2025

First commit by essentialplugin account. Version 2.6.7 plants the unserialize() RCE backdoor. Changelog lies: ‘Check compatibility with WordPress version 6.8.2.’

August 30, 2025

essentialplugin.com WHOIS updated to ‘Kim Schmidt’ in Zurich, with a ProtonMail address.

April 5-6, 2026

Backdoor weaponized. analytics.essentialplugin.com begins distributing malicious payloads to all sites running these plugins.

April 7, 2026

WordPress.org Plugins Team permanently closes all 31 essentialplugin plugins in a single day.

April 8, 2026

WordPress.org forces auto-update to v2.6.9.1 across all sites. Adds return; statements and comments out the @$clean() backdoor line.

The buyer’s very first SVN commit was the backdoor.

WordPress.org closed 30+ plugins in a single day.

On April 7, 2026, the WordPress.org Plugins Team permanently closed every plugin from the Essential Plugin author. At least 30 plugins, all on the same day. Here are the ones I confirmed:

- Accordion and Accordion Slider — `accordion-and-accordion-slider`
- Album and Image Gallery Plus Lightbox — `album-and-image-gallery-plus-lightbox`
- Audio Player with Playlist Ultimate — `audio-player-with-playlist-ultimate`
- Blog Designer for Post and Widget — `blog-designer-for-post-and-widget`
- Countdown Timer Ultimate — `countdown-timer-ultimate`
- Featured Post Creative — `featured-post-creative`
- Footer Mega Grid Columns — `footer-mega-grid-columns`
- Hero Banner Ultimate — `hero-banner-ultimate`
- HTML5 VideoGallery Plus Player — `html5-videogallery-plus-player`
- Meta Slider and Carousel with Lightbox — `meta-slider-and-carousel-with-lightbox`
- Popup Anything on Click — `popup-anything-on-click`
- Portfolio and Projects — `portfolio-and-projects`
- Post Category Image with Grid and Slider — `post-category-image-with-grid-and-slider`
- Post Grid and Filter Ultimate — `post-grid-and-filter-ultimate`
- Preloader for Website — `preloader-for-website`
- Product Categories Designs for WooCommerce — `product-categories-designs-for-woocommerce`
- Responsive WP FAQ with Category — `sp-faq`
- SlidersPack – All in One Image Sliders — `sliderspack-all-in-one-image-sliders`
- SP News And Widget — `sp-news-and-widget`
- Styles for WP PageNavi – Addon — `styles-for-wp-pagenavi-addon`
- Ticker Ultimate — `ticker-ultimate`
- Timeline and History Slider — `timeline-and-history-slider`
- Woo Product Slider and Carousel with Category — `woo-product-slider-and-carousel-with-category`

- WP Blog and Widgets — `wp-blog-and-widgets`
- WP Featured Content and Slider — `wp-featured-content-and-slider`
- WP Logo Showcase Responsive Slider and Carousel — `wp-logo-showcase-responsive-slider-slider`
- WP Responsive Recent Post Slider — `wp-responsive-recent-post-slider`
- WP Slick Slider and Image Carousel — `wp-slick-slider-and-image-carousel`
- WP Team Showcase and Slider — `wp-team-showcase-and-slider`
- WP Testimonial with Widget — `wp-testimonial-with-widget`
- WP Trending Post Slider and Widget — `wp-trending-post-slider-and-widget`

All permanently closed. The author search on WordPress.org returns zero results. The `analytics.essentialplugin.com` endpoint now returns `{"message":"closed"}`.

This has happened before.

In 2017, a buyer using the alias “Daley Tias” purchased the Display Widgets plugin (200,000 installs) for $15,000 and injected payday loan spam. That buyer went on to compromise at least 9 plugins the same way.

The Essential Plugin case is the same playbook at a larger scale. 30+ plugins. Hundreds of thousands of active installations. A legitimate 8-year-old business acquired through a public marketplace and weaponized within months.

I patched every affected plugin in my fleet.

WordPress.org’s forced update added `return;` statements to disable the phone-home functions. That is a band-aid. The `wpos-analytics` module is still there with all its code. I built patched versions with the entire backdoor module stripped out.

I scanned my entire fleet and found 12 of the 26 Essential Plugin plugins installed across 22 customer sites. I patched 10 of them (one had no backdoor

module, one was a different “pro” fork by the original authors). Here are the patched versions, hosted permanently on B2:

```
# Countdown Timer Ultimate
wp plugin install https://plugins.captaincore.io/countdown-timer-ultimate-2.6.9.

# Popup Anything on Click
wp plugin install https://plugins.captaincore.io/popup-anything-on-click-2.9.1.1

# WP Testimonial with Widget
wp plugin install https://plugins.captaincore.io/wp-testimonial-with-widget-3.5.

# WP Team Showcase and Slider
wp plugin install https://plugins.captaincore.io/wp-team-showcase-and-slider-2.8

# WP FAQ (sp-faq)
wp plugin install https://plugins.captaincore.io/sp-faq-3.9.5.1-patched.zip --fo

# Timeline and History Slider
wp plugin install https://plugins.captaincore.io/timeline-and-history-slider-2.4

# Album and Image Gallery plus Lightbox
wp plugin install https://plugins.captaincore.io/album-and-image-gallery-plus-li

# SP News and Widget
wp plugin install https://plugins.captaincore.io/sp-news-and-widget-5.0.6-patche

# WP Blog and Widgets
wp plugin install https://plugins.captaincore.io/wp-blog-and-widgets-2.6.6.1-pat

# Featured Post Creative
wp plugin install https://plugins.captaincore.io/featured-post-creative-1.5.7-pa

# Post Grid and Filter Ultimate
wp plugin install https://plugins.captaincore.io/post-grid-and-filter-ultimate-1
```

Each patched version removes the entire `wpos-analytics` directory, deletes the loader function from the main plugin file, and bumps the version to `-patched`. The plugin itself continues to work normally.

If you have an Essential Plugin plugin I did not patch, you can do it yourself.

The process is straightforward with Claude Code. Point it at this article for context, tell it which plugin you need patched, and it can strip the `wpos-analytics` module the same way I did. The pattern is identical across all of the Essential Plugin plugins:

1. Delete the `wpos-analytics/` directory from the plugin
2. Remove the loader function block in the main plugin PHP file (search for "Plugin Wpos Analytics Data Starts" or `wpos_analytics_anl`)
3. Bump the `Version:` header to add `-patched`
4. Zip and install with `wp plugin install your-plugin-patched.zip --force`

Check your wp-config.php

The malware appends itself on the same line as `require_once ABSPATH . wp-settings.php;` so it is easy to miss with a quick glance. If your file is significantly larger than expected (the injected payload adds about 6KB), the site was actively compromised and needs a full cleanup beyond just patching the plugin.

The WordPress plugin marketplace has a trust problem.

Two supply chain attacks in two weeks. Both followed the same pattern. Buy a trusted plugin with an established install base, inherit the WordPress.org commit access, and inject malicious code. The Flippa listing for Essential Plugin was public. The buyer's background in SEO and gambling marketing was public. And yet the acquisition sailed through without any review from WordPress.org.

WordPress.org has no mechanism to flag or review plugin ownership transfers. There is no "change of control" notification to users. No additional code review triggered by a new committer. The Plugins Team responded quickly once the attack was discovered. But 8 months passed between the backdoor being planted and being caught.

If you manage WordPress sites, search your fleet for any of the 26 plugin slugs listed above. If you find one, patch it or remove it. And check wp-config.php.

PREVIOUS

How CaptainCore Drift Uncovered a Nulled Plugin Ring

NEXT

1,600 Emails in One Conversation: How I Triage My Inbox With Claude Code