



# G DATA Whitepaper 2018/01

## Analysis of Script.Backdoor.Wp-Vcd.A

Analysis by:  
<https://twitter.com/RansomBleed>



# Contents

<b>1. Introduction.....</b>	<b>3</b>
<b>2. Spreading routine.....</b>	<b>3</b>
<b>3. Core functionality.....</b>	<b>4</b>
<b>4. Further research .....</b>	<b>5</b>
<b>5. Website statistics.....</b>	<b>6</b>
<b>6. Final words .....</b>	<b>7</b>
<b>7. File hashes and resources .....</b>	<b>8</b>

# 1. Introduction

Wordpress is the most widely used CMS (content management system) out there. The easy installation and configuration as well as the tons of plugins and themes out there – which are almost eliminating the need to program - makes Wordpress a popular choice for beginners as well as experts. This makes it a favorite platform to target for criminals as well, because the criminals can attack more people compared to targeting a less frequently used CMS. In the last months there has been a new malware campaign spreading around. You find a link to previous insights about the wp-vcd malware [here\[1\]](#). However, the Wp-Vcd backdoor has evolved and this report clarifies the new advancements of the backdoor and further information about the author. Wp-vcd is hiding itself in pirated Wordpress themes. The pirated themes can be found on several websites via the Google search. When installed, Wp-vcd will compromise the systems of webmasters who are not willing to pay for the work of a developer.

# 2. Spreading routine

Initially the backdoor was found by downloading the theme ExProduct v1.0.7[2] from the site “hxxp://downloadfreethemes.download”. This website is hosting a lot of pirated Wordpress themes. At the time of writing, the site was hosting 32.200 themes.

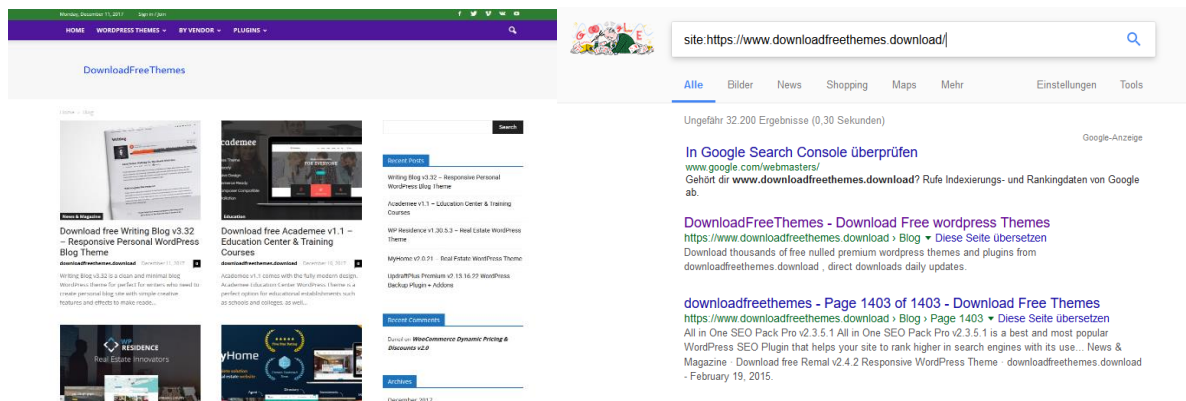


Figure 1. left: Index page. Right: Search results count

If for example one searches for “Download free Adventure Tours v3.1.8”, the very first result in Google will point to the malicious site. Interestingly, the author let the Wordpress uploads folder visible to the public. This led me to the other sites the author is actively using to get new installations. Here is a list of them:

- 24x7themes.top
- Dlword.press
- Freenulled.top
- Freethemes.space
- Null5.top
- Themesdad.com
- Wpmania.download

At first glance, there doesn't seem to be a difference on those websites besides the different logo. If you look closely, it is clear that the author uses title variations for posts on those websites. The author's objective is to generate more page visits overall, since different keywords are being used. As you may know, an important ranking factor of Google and other search engines, which determine on which position a website should appear in the search results, are keywords. Because people type in different search terms in order to find what they want, the author uses one site for a specific kind of search query and another site for another query.

**For example:**

<https://wpmania.download>

➔ “Writing Blog v3.32 – Responsive Personal WordPress Blog Theme”

<https://www.downloadfreethemes.download/>

➔ “Download free Writing Blog v3.32 – Responsive Personal WordPress Blog Theme”

### 3. Core functionality

Once the theme is installed, a piece of *base64* encrypted code, which is stored inside the „class.theme-modules.php“, is placed at the end of the theme file `functions.php`. Whenever any file that uses `functions.php` is called (except “wp-cron.php” and “xmlrpc.php”) it will download PHP code located at “hxxp://linos.cc/code.php” and store it into “wp-includes/wp-tmp.php”. This code is then loaded using the `include` function. After the code has been loaded, the content of `wp-tmp.php` gets deleted. A small piece of the code can be seen in Figure 2. As you can probably see, this code is being used to display advertisements, since HTML script tags are being used which embed URLs that distinctively look like they are associated with advertising.



```

ini_set('display_errors', 0);
error_reporting(0);
$wp_auth_key='7af507a87318d795efbdb0e3a9028aad';

if ( ! function_exists( 'slider_option' ) ) {
function slider_option($content){
if(!is_single())
{

$con = '
';
$con2 = '
<script type="text/javascript" src="//go.oclasrv.com/apu.php?zoneid=1494052"></script>
<script async="async" type="text/javascript" src="//go.mobisla.com/notice.php?p=1494054&interactive=1&pushup=1"></script>
';
$content=$content.$con2;
}
return $content;
}

function slider_option_footer(){
if(!is_single())
{

```

Figure 2. Part of the downloaded code

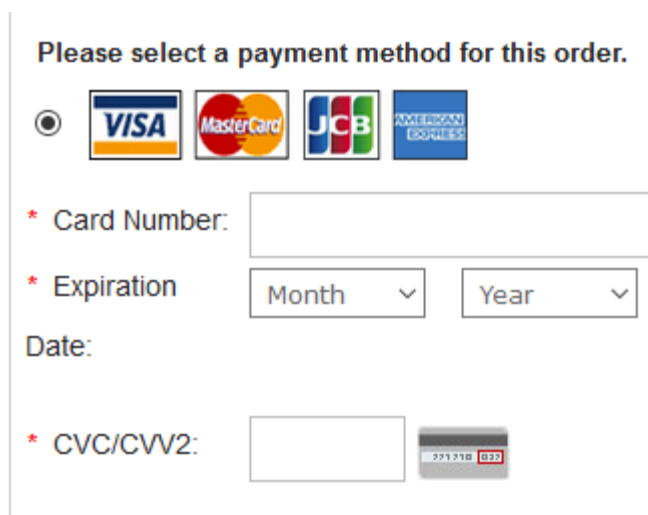
The newly added code of the `functions.php` file has the ability to change the `functions.php` file itself, if specific GET parameters are listed.

**?action=change\_domain&newdomain=** When this parameter is called with functions.php, the domain from where the functions.php is getting the PHP code (hxxp://linos.cc) is getting changed to a new domain.

**?action=change\_code&newcode=** Inside the functions.php file there is a placeholder for code which can be added in future. By using this parameter new code is placed to that location.

## 4. Further research

Inside the public uploads folder of the website “hxxp://downloadfreethemes.download”, a logo with the writing “quickloansnow.co.uk” can be found. If visiting this page, a shop for shoes can be seen. I doubt that it’s likely, that the author of that page will actually deliver the offered shoes. It’s more likely that the author wants to get shopping information like the billing address and credit card data from people visiting the page, since the author also seem not to care about infecting people’s websites with backdoors. In figure 3. below you can see the form to fill out the credit card information.



Please select a payment method for this order.

VISA  MasterCard  JCB  AMERICAN EXPRESS

\* Card Number:

\* Expiration

Date:


\* CVC/CVV2:  

Figure 3. Credit card form

The WHOIS entry of “hxxp://quickloansnow.co.uk” returns the name “Hamzat Atta” from London. Facebook returns two possible candidates when searching with this information, which can be seen here “https://www.facebook.com/public/Hamzat-Atta”. We can speculate whether one of those two is the author behind those websites.

A reverse search of WHOIS registrant names reveals five more hosts, which are also shopping websites. The sites are listed below:

- Golago.co.uk
- Goplanb.co.uk
- Mjironing.co.uk
- Rhymestars.co.uk
- Sample-website.co.uk

Those websites are most likely fraudulent websites, since they are obviously being posted on other websites to achieve a higher ranking and more visibility on the web. Legit sites are doing this too, but they aren't spamming their links over all possible places. Convince yourself with the Google search query "intext:goplanb.co.uk -site:goplanb.co.uk". You can easily see in the search results, that the sites listed have clearly nothing to do with the website goplanb.co.uk.

## 5. Website statistics

According to the free website analysis site "http://similarweb.com", the domain "hxxp://downloadfreethemes.download" had 880.000 total visits in the month of January alone!

As you can see from the previous months in figure 4. the traffic is growing by every month and could reach 1 million in February already. If only 1% of those 1 million people actually download themes and use it on their personal website, the author is having 10.000 new infected hosts per month and growing. In reality, this number could be much higher of course.

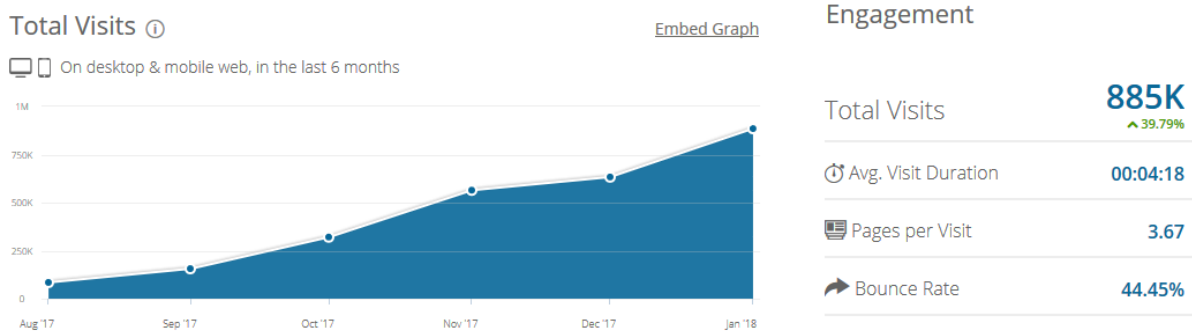
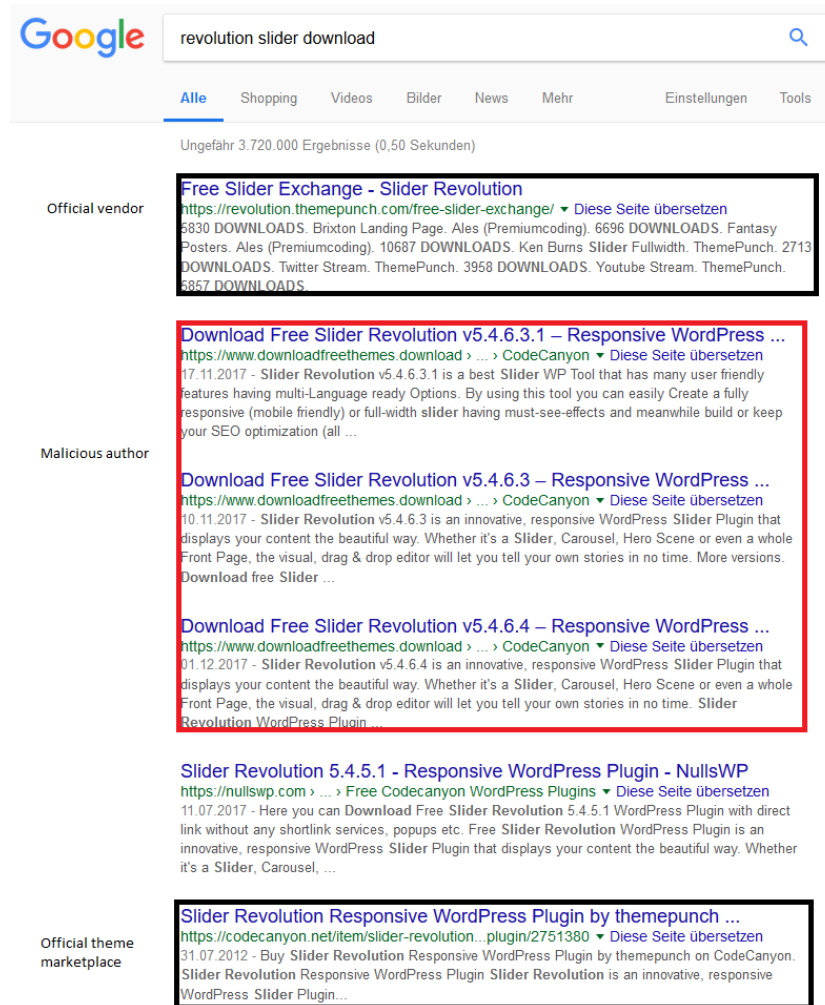


Figure 4. downloadfreethemes.download estimated traffic

As mentioned before, the author is trying to get people to visit his malicious pages using search engine optimization. His goal is to rank as high in the search results as possible, since people tend to click on the first page results only with each result being less clicked from the top to the bottom of the page. According to similarweb, 80% of the traffic comes from search queries. This is getting crystal clear when searching for "revolution slider download" in Google. Ridiculously, the malicious website even ranks higher than an official template selling website(codecanyon.net), as you can see in figure 5. below. At least he isn't ranking higher than the vendor, which created the software.

This example shows, that Google isn't perfect and can be tricked into displaying unwanted results. Therefore, the antivirus solution has to take care of those problems. The average user doesn't know and doesn't even want to know about all kinds of dangers out there. Just like there are criminals at the street robbing people, there are bodyguards protecting those people. GDATA and many other antivirus companies are the "bodyguards of the internet" keeping people secure from online criminals, which are in most cases even more disturbing than a person on the street stealing your purse.



The screenshot shows a Google search for "revolution slider download". The search results are categorized into three groups:

- Official vendor:** A result from "Free Slider Exchange - Slider Revolution" with a URL pointing to <https://revolution.themepunch.com/free-slider-exchange/>. It lists various download statistics for different themes.
- Malicious author:** Two results from "Download Free Slider Revolution v5.4.6.3.1 - Responsive WordPress ..." and "Download Free Slider Revolution v5.4.6.3 - Responsive WordPress ...". Both results mention "CodeCanyon" and describe the plugin as a "best Slider WP Tool" or "innovative, responsive WordPress Slider Plugin".
- Official theme marketplace:** A result from "Slider Revolution Responsive WordPress Plugin by themepunch ..." with a URL pointing to <https://codecanyon.net/item/slider-revolution...plugin/2751380>.

Figure 5. Example search query

## 6. Final words

Visiting the internet can be an experience with lots of pleasure and joy. Social media allows us to be connected with everyone at any time, leading to a much faster exchange of wisdom or cute kittens all over the world. However, visiting the wrong places online can lead to unwanted results like having malware installed on the private homepage for the local hair stylist website you always wanted. As long as people almost blindly trust any online presence they see, people are getting targeted and this won't stop anytime soon. Google is a trusted company in the eyes of many people, since they reliably deliver search results and mails since several years. Criminals know that very well, hence the amount of programs like "paypal generator v1.0" or "Facebook hacker v2.3 updated" can be found with search engines like Google. In the case of this report, the criminal is targeting people who need Wordpress themes for free. In this rough game, which is having more shady criminals than white knights, The GDATA team is doing the absolute best to protect customers from being a potential target of various types of criminals online. Stay safe!



## 7. File hashes and resources

[1] <https://www.bleepingcomputer.com/news/security/wp-vcd-wordpress-malware-spreads-via-nulled-wordpress-themes/>

[2] a70f9b23b71f94a81788a277b8fb39f3d271a637e5ad1be3b0d9f45d575726da

If you want to stay updated about malware, be sure to follow these accounts:

[RansomBleed](#) - My personal twitter account about the latest malware reports.

[GDataSoftwareAG](#) - G DATAs twitter company account.

[Blog](#) - The G DATA blog about all kinds of security-related news.