Скрытые ссылки, к сожалению, **на страницах сайта** иногда встречаются, таким образом непорядочные веб мастера пытаются продвигать сайты. Ведь чем больше ресурсов в интернете ссылаются на сайт, тем больше поисковые системы считают, что сайт полезен пользователям информационного пространства. Такие приёмы хороши (для редисок) до поры до времени, а вот Вашему сайту, на котором такие ссылки появились ничего хорошего не светит. Если вовремя не обнаружить такие замаскированные **вредоносные ссылки** , Ваш драгоценный сайт запросто вылетит из индекса и вернуть его обратно будет нелегко. Только представьте себе, если на каждой странице будет одна или две скрытых ссылок, а бывает и того больше, да ещё и ссылаться они будут на сайты с плохой репутацией?

Откуда берутся невидимые ссылки?

Варианты их появления разные, смысл один - спам или просто вредительство. Причины появления таких ссылок может быть взлом сайта через уязвимость в системе или sql инъекцию (специальный запрос в базу данных, вызывающий ошибку), сборка джумлы загруженная не с официального сайта, шаблон сайта, скачанный опять же не с сайта разработчика, недобросовестный хостер, который решил на Вас поездить, вирусы на машине с которой подключаетесь к ftp аккаунту, к административной панели, не правильное назначение прав доступа к папкам и файлам сайта. Хотите найти и наказать злодея, который Вам такое устроил - посмотрите лог-файлы через сервисы статистики, обратитесь к хостеру, может выясните ip адрес, но как правило это пустая трата времени. Лучше не теряя времени приступить к лечению сайта, пока зараза не развилась до других, более серьёзных масштабов.

Как обнаружить скрытые ссылки?

Способ первый - открыть исходный код страницы и просмотреть всю страницу и все ссылки. Поле поиска, вводим "http://" и вперед просматривать код. Довольно долгая песня, но тем не менее найти ссылку, если она есть можно. Способ второй - для интернет браузера Mozilla Firefox имеется замечательное дополнение **RDS Bar** . Установив его, можно всегда получить подробную информацию об открытой странице.

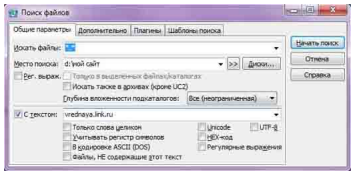
Сколько страниц в индексе поисковых страниц, возраст сайта, ТИЦ и PR, счетчики посещаемости, количество внешних и внутренних ссылок и ещё многое и многое другое. Раз уж мы в этой статье говорим о ссылках, то нас интересует в данный момент их тип и количество. Кликнув на "Links", можно получить подробный отчет о всех ссылках на странице.

Найти и обезвредить!

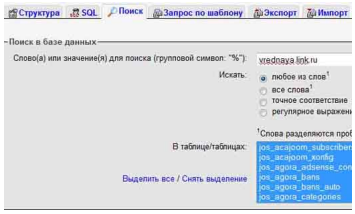
Если уж так случилось, что у Вас на страницах сайта завелись паразиты, их нужно гнать поганой метлой. И чем быстрее, тем лучше для здоровья и репутации Вашего сайта. Как они туда забрались пока разбираться некогда, хотя пароли на доступ к сайту следует поменять сразу, - на случай взлома сайта, предварительно тщательно проверив антивирусом компьютер, с которого Вы осуществляете доступ к ресурсу.

Где искать скрытые ссылки?

Если ссылка не особо сильно запрятана, для начала стоит заглянуть в шаблон Вашего сайта. Файл **default.php** можно найти по пути **templatesназвание шаблонadefaults.php**. Откройте файл и внимательно просмотрите его, вполне возможно, но это редко, что Вы сразу найдете злополучную ссылку и удалите её. Если нет, не отчаиваемся и копируем на локальный компьютер все папки сайта. Проверьте все скопированные каталоги антивирусом. С помощью
Total Commander
(есть и другие программы) можно выполнить поиск в содержимом файлов на предмет встречающихся слов во всех каталогах, включая все подкаталоги всех уровней вложенности.



Введите часть адреса вредной паразитарной ссылки и нажмите "Начать поиск". Если паразит встречается в содержимом файлов Вашего сайта, останется открыть найденные страницы и ампутировать злокачественную опухоль. Не нашли? Не падайте духом! Следующее место поиска это **база данных сайта**. Заходите в **phpMyAdmin**, выберите базу данных и нажмите "Поиск". Розыск возможно выполнить по всем таблицам. Находим и удаляем.



Если скрытую ссылку так и не удалось найти

Ну что ж, есть ещё один проверенный способ. Уж он то точно должен помочь. Суть его заключается в том, чтобы перезаписать файлы Joomla из дистрибутива поверх файлов джумлы на хостинге. Первое, что Вы непременно должны сделать это резервную копию базы данных (хоть она и не затрагивается в этой процедуре, но всё таки сделайте, мало ли что) и резервную копию сайта. Загрузите с официального сайта разработчиков Joomla дистрибутив той же версии, что установлен у Вас. Перезалить нужно будет поверх уже существующих каталогов все файлы, за исключением папок **installation**, **cache** и **templates**. Не нужно также перезаписывать файл глобальной конфигурации **configuration.php** и файл дополнительной конфигурации веб сервера Apache **.htaccess**.

Устранение последствий и как защитить сайт от взлома

- Проверьте корневую директорию сайта на предмет наличия в ней подозрительных и лишних скриптов;
- Все расширения, которые Вы используете обновите до актуальных версий;
- Все расширения, которые Вы не используете удалите;
- Удалите всех администраторов кроме себя и смените пароль. Можно поменять и логин, очень часто все пользуются именем admin. Не зная логина злоумышленнику сложней будет взломать сайт, чем не зная только пароль. Не поскупитесь на количество символов пароля и постарайтесь чтобы он получился придуманным нигде в лексиконе не встречающимся словом. Нигде не храните пароль, не пользуйтесь менеджерами хранения паролей и никому не говорите его;
- Поменяйте пароль доступа к FTP серверу;
- Не ленитесь раз в неделю сканировать компьютер антивирусом, а иногда другим антивирусом, не тем к которому привыкли как бы авторитетно и лестно о нём не отзывались пользователи. Один антивирус хорошо, а два лучше;
- ОБЯЗАТЕЛЬНО делайте резервные копии баз данных и файлов сайта, храните несколько версий (разные даты копий). Хранить резервные копии желательно на разных носителях информации. Если с одним что случится, другой есть в резерве. Лучше быть параноиком, чем что-то упустить :-)

А ещё встречается следующая жуткая штука: код-фантом

Яндекс вебмастер ругается, что на сайте обнаружен вредоносный код. Через 2-3 дня поисковик считает, что вирус на сайте удален и все нормально. А еще через 2-3 дня снова его находит. Гугл молчит, все в порядке. Проверка файлов сайта антивирусами ничего не даёт. Код сам появляется и сам пропадает. Речь идет о Troj/Iframe-IW, он же Trojan-Downloader.HTML.Agent.wy. Лечение: сравните оригинальный джумловский файл librariesjoomlautilitiescompatcompat.php с Вашим. Разное содержание? Перезалейте compat.php оригинальным.

Всего Вам доброго!

//