Recently my Joomla 1.7 site was hacked. I knew nothing about this. The site worked fine. But when i did some test search with Google and found that the site is found with keywords that are not used in my site. When i looked at Google cache i was impressed that there are different pages. Contents of my pages was replaced with advertising links and texts.

This was some sort of cloaking. And this meant my Joomla site is infected with something bad.

I already sow similar problem for my another Joomla 1.5 site year ago. So this time i know what to do.

1. **Block access to the bot on the site.**

After quick look on site folders i found that there is folder components/downloads. It is not usual folder for Joomla. Inside this folder i found PHP file with strange contents. "define("thrnutm", "65c756b2f3019890375e66f239328727"); $GLOBALS['_1516428634_']=Array(.....". Definitely this is not part of Joomla. I have removed that file. But is this the only such file inside Joomla folders?

I decided to block access to all PHP files that are different from index.php in Joomla root.

I created small PHP script:

{codecitation style="brush:php;"}<?php

$s=$_SERVER['REQUEST_URI'];

```
$h=fopen('../cache/d.txt','a');
fwrite($h,'['.date('d-m-Y H:i:s').']: '.$s."n");
fwrite($h,print_r($_REQUEST,true)."n");
fwrite($h,print_r($_SERVER,true)."n");
fclose($h);

?>{/codecitation}
```

And put it in file components/stop.php

Also i have done change in file .htaccess . I have added:

```
{codecitation}

RewriteCond %{REQUEST_URI} !^/administrator/index

RewriteCond %{REQUEST_URI} !^/components/stop.php
RewriteRule ^(.+/.+.php)$ /components/stop.php/$1 [L]

{/codecitation}
```

After this i was able to see all direct requests to php files that are different from index.php in file cache/d.txt and i located that files.

2. **The problem is still there.**

In folder components/downloads there was also file .htaccess with contents:

{codecitation}

```
RewriteEngine On
RewriteBase /components/downloads

RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f

RewriteRule index.php.* - [L]

RewriteCond %{REQUEST_FILENAME} !-d
RewriteCond %{REQUEST_FILENAME} !-f

RewriteRule ^(.*) index.php?id=$1
```

{/codecitation}

This means that hacker can access and configure his bot with URIs that don't contain .php extension and my protection will not help.

I had to find all .htaccess files in Joomla folders and delete them.

3. **Find all infections.**

I downloaded my Joomla site files to local drive and did search with text "$GLOBALS". There were near 10 not Joomla files with such text. Totally there were 3 types of scripts. All of them can be used to do everything with site files/folders and have full control of the site.

4. **How the site was infected.**

This is most interesting question. It is needed to find how initially your site was infected.

In did this with following way:

- Collect IP addresses that were used to access PHP scripts directly and collected in cache/d.txt file.

- Use found files to find what else requests were done from them to your site . Find IPs in access logs to your site (apache logs or something). Usually your will see some strange request with SQL instructions in it.

In my case i found that the site was hacked using SQL injection. One of installed components had bug.

5. **Summary.**

After fixing of bug in component and disabling pf direct access to PHP files in Joomla folders my site was fixed.