# antileech - Module to protect images from direct downloading on your site - Modules

NEWS_PDF_AUTHOR: andrey3761

NEWS_PDF_DATE: 2009/5/1 21:30:00

Many sites, in attempt to save their bandwidth steal images from others sites, placed links to images on their pages directed to other sites, where the actual images were located.

To protect your content from thieves, we made this module. This Module replace images if HTTP header field 'Referer' did not match with yours site URL. Module support white list allows for direct downloading by "freinds"( or search engines) IPs or domains listed in .htaccess file.

**Features:**
* Shows thieves sites, where your images are displayed as their own, but are physically located on your site.
* Shows page of referrer, where displayed images from your site are.
* Shows HTTP header fields of end clients who are trying to access stolen from your site images.
* On the fly, replaces requested file with antileech image(show them something like "This image was stolen from http://yoursite.tld...".
* Shows requsted file.

**Requirements:**
* HTTP server - Apache with installed module ModRewrite.
* Graphics library - GD.
* PHP version > 4.x.x

XOOPS Russian support 2 (XOOPS2.ru)

Download antileech

**Installation:**
Install module as usual, by uploading directory "antileech" to directory "modules" on your site.
Install module on admin side in the same way as other modules.
Set option "Enable log" in module's preference if you need it.
Switch to "Images" menu and upload from there image that would be shown to clients instead of original requested image file.
In a module configuration specify title of page and the displayed text at protection of files against direct loading
In the root of your site (XOOPS_ROOT_PATH) place the following into the file .htaccess
(Make changes to directories and URLs as you needed)

```
#
#--------------------------------------------------------------------------------
#
# If already exists, then skip the next line
RewriteEngine on

# Root of your site. If already exist, then skip next statment "RewriteBase ...."
# If your site is located in DOCUMENT_ROOT then leave RewriteBase /
# If your site is located in subdirectory of DOCUMENT_ROOT (such as /en ),then change to actual value
# RewriteBase /en

# Protection of images
# Enable direct downloading if field REFERER is empty(usually it is search engines)
RewriteCond %{HTTP_REFERER} !^$
# Enable own site and its all subdomains
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?(subdomain1\.|subdomain2\.)?yoursite\.com/ [NC]
# Enable direct downloading for trusted sites(white list)
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?freindssite1\.com/ [NC]

# (uploads|folder1|folder2) - list of directories to protect, where antileech track access and protect images
# (jpg|jpeg|png|gif) - list of extensions that should be protected
RewriteRule (uploads|folder1|folder2)/(.*)\.(jpg|jpeg|png|gif)$ /modules/antileech/img\.php [NC]

# Protection of files
# Enable direct downloading if field REFERER is empty(usually it is search engines)
RewriteCond %{HTTP_REFERER} !^$
# Enable own site and its all subdomains
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?(subdomain1\.|subdomain2\.)?yoursite\.com/ [NC]
# Enable direct downloading for trusted sites(white list)
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?freindssite1\.com/ [NC]

# (uploads|folder1|folder2) - list of directories to protect, where antileech track access and protect files
# (djvu|pdf|rar|zip) - list of extensions that should be protected
RewriteRule (uploads|folder1|folder2)/(.*)\.(djvu|pdf|rar|zip)$ /modules/antileech/file\.php [NC]



#
#--------------------------------------------------------------------------------
#
```

Many sites, in attempt to save their bandwidth steal images from others sites, placed links to images on their pages directed to other sites, where the actual images were located.

To protect your content from thieves, we made this module. This Module replace images if HTTP header field 'Referer' did not match with yours site URL. Module support white list allows for direct downloading by "freinds"( or search engines) IPs or domains listed in .htaccess file.

**Features:**
* Shows thieves sites, where your images are displayed as their own, but are physically located on your site.
* Shows page of referrer, where displayed images from your site are.
* Shows HTTP header fields of end clients who are trying to access stolen from your site images.
* On the fly, replaces requested file with antileech image(show them something like "This image was stolen from http://yoursite.tld...".
* Shows requsted file.

**Requirements:**
* HTTP server - Apache with installed module ModRewrite.
* Graphics library - GD.
* PHP version > 4.x.x

XOOPS Russian support 2 (XOOPS2.ru)

Download antileech

**Installation:**
Install module as usual, by uploading directory "antileech" to directory "modules" on your site.
Install module on admin side in the same way as other modules.
Set option "Enable log" in module's preference if you need it.
Switch to "Images" menu and upload from there image that would be shown to clients instead of original requested image file.
In a module configuration specify title of page and the displayed text at protection of files against direct loading
In the root of your site (XOOPS_ROOT_PATH) place the following into the file .htaccess
(Make changes to directories and URLs as you needed)

```
#
#---------------------------------------------------------------------------
#
# If already exists, then skip the next line
RewriteEngine on

# Root of your site. If already exist, then skip next statment "RewriteBase ...."
# If your site is located in DOCUMENT_ROOT then leave RewriteBase /
# If your site is located in subdirectory of DOCUMENT_ROOT (such as /en ),then change to
actual value
# RewriteBase /en

# Protection of images
# Enable direct downloading if field REFERER is empty(usually it is search engines)
RewriteCond %{HTTP_REFERER} !^$
# Enable own site and its all subdomains
RewriteCond %{HTTP_REFERER}
!^https?://(www\.)?(subdomain1\.|subdomain2\.)?yoursite\.com/ [NC]
# Enable direct downloading for trusted sites(white list)
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?freindssite1\.com/ [NC]

# (uploads|folder1|folder2) - list of directories to protect, where antileech track access and
protect images
# (jpg|jpeg|png|gif) - list of extensions that should be protected
RewriteRule (uploads|folder1|folder2)/(.*)\.(jpg|jpeg|png|gif)$ /modules/antileech/img\.php [NC]

# Protection of files
# Enable direct downloading if field REFERER is empty(usually it is search engines)
RewriteCond %{HTTP_REFERER} !^$
# Enable own site and its all subdomains
RewriteCond %{HTTP_REFERER}
!^https?://(www\.)?(subdomain1\.|subdomain2\.)?yoursite\.com/ [NC]
# Enable direct downloading for trusted sites(white list)
RewriteCond %{HTTP_REFERER} !^https?://(www\.)?freindssite1\.com/ [NC]

# (uploads|folder1|folder2) - list of directories to protect, where antileech track access and
protect files
# (djvu|pdf|rar|zip) - list of extensions that should be protected
RewriteRule (uploads|folder1|folder2)/(.*)\.(djvu|pdf|rar|zip)$ /modules/antileech/file\.php [NC]



#
#------------------------------------------------------------------------------
#
```