Ce script va scanner l'ensemble de votre site à la recherche de quelques 'signatures' (patterns) de virus *(pour des raisons 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.

×Quelques considérations à bien comprendre :

1. Le scan est superficiel et en aucun cas exhaustif; seules quelques signatures sont recherchées alors que les possibilités de hack sont fort nombreuses,
2. si le script détecte la présence de certaines signatures (p.ex. "base64\_decode"), cela n'implique pas que votre site ait été hacké. En effet, certaines instructions sont utilisées lors de hack (base64\_decode) mais sont également utilisées de manière parfaitement légitime dans des codes sources php,
3. Les résultats retournés doivent **TOUJOURS** être correctement compris avant de prendre une quelconque action, demandez de l'aide sur un forum p.ex. si vous doutez.
4. Soyez patient : le scan se fait fichier par fichier et peut donc être plus ou moins long; dépendant de la complexité de votre site.

L'auteur du script décline toute responsabilité en cas de mauvais usage du script ou d'actions prises par le webmaster suite aux résultats mentionnés.

1. Nettoyé 2. 8.623 fichiers 3. Scanner le site  4. Supprimer ce script du serveur

8.623 fichiers vont être analysés (1.818 fichiers ont été ignorés car ils sont repris sur la liste blanche d'aeSecure et 17.507 ignorés comme paramétré dans l'écran des options avancées).

1 -> 500 501 -> 1.000 1.001 -> 1.500 1.501 -> 2.000 2.001 -> 2.500 2.501 -> 3.000 3.001 -> 3.500 3.501 -> 4.000 4.001 -> 4.500 4.501 -> 5.000 5.001 -> 5.500 5.501 -> 6.000 6.001 -> 6.500 6.501 -> 7.000 7.001 -> 7.500 7.501 -> 8.000 8.001 -> 8.500 8.501 -> 8.623

8623 fichiers ont été analysés dont 193 sont détectés comme potentiellement dangereux.  
1 fichiers ont été ignorés car ayant une taille supérieure ou égale à 1 MB et 0 fichier(s) inaccessible(s) à cause d'un niveau de permission (chmod) trop restreint.

Si les résultats de ce script ont démontré la présence de virus, veuillez bien comprendre que le script a cherché des fichiers connus comme malsain (blacklist) et qu'il a recherché qu'un tout petit nombre de possibilités de hacking. Seules quelques signatures; simples; ont été recherchées. Il faut donc vous attendre à ce que vous ayez d'autres virus sur votre site web et il faudrait considérer un scan complet du site pour les éliminer. N'hésitez pas à me contacter : [https://www.avonture.be](https://www.avonture.be/), je peux nettoyer votre site web.

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_admin\script.php*(174.63K)(Date dernière modif. August 27 2024 02:31:12.)*aca529635c9d725e1d1bf0d08ac6d198**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **108157** du fichier; voici le contexte :
2. '/media/vendor/codemirror/mode/meta.min.js.gz',
3. '/media/vendor/codemirror/mode/**mirc**/**mirc**.js',
4. '/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js',

'/media/vendor/

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **108162** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/meta.min.js.gz',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js',

'/media/vendor/codem

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **108215** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**mirc**/**mirc**.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js.gz',

'/media/

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **108220** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**mirc**/**mirc**.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js.gz',

'/media/vendo

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **108277** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js.gz',

'/media/vendor/codemirror/mode/mllike/mllike.js',

'/media/

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **108282** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js',

'/media/vendor/codemirror/mode/**mirc**/**mirc**.min.js.gz',

'/media/vendor/codemirror/mode/mllike/mllike.js',

'/media/vendo

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mirc**Trouvé en position **152778** du fichier; voici le contexte :

ca',

'/media/vendor/codemirror/mode/mllike',

'/media/vendor/codemirror/mode/**mirc**',

'/media/vendor/codemirror/mode/mbox',

'/media/vendor/codemirror/mode/math

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **111027** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/pig/pig.min.js.gz',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **111038** du fichier; voici le contexte :

ndor/codemirror/mode/pig/pig.min.js.gz',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js',

'/media/

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **111097** du fichier; voici le contexte :

a/vendor/codemirror/mode/power**shell**/power**shell**.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js.gz',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **111108** du fichier; voici le contexte :

demirror/mode/power**shell**/power**shell**.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js.gz',

'

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **111171** du fichier; voici le contexte :

ndor/codemirror/mode/power**shell**/power**shell**.min.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js.gz',

'/media/vendor/codemirror/mode/properties/properties.js',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **111182** du fichier; voici le contexte :

rror/mode/power**shell**/power**shell**.min.js',

'/media/vendor/codemirror/mode/power**shell**/power**shell**.min.js.gz',

'/media/vendor/codemirror/mode/properties/properties.js',

'/med

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **113937** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/scheme/scheme.min.js.gz',

'/media/vendor/codemirror/mode/**shell**/**shell**.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js',

'/media/vend

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **113943** du fichier; voici le contexte :

a/vendor/codemirror/mode/scheme/scheme.min.js.gz',

'/media/vendor/codemirror/mode/**shell**/**shell**.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js',

'/media/vendor/cod

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **113997** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**shell**/**shell**.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js.gz',

'/med

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **114003** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**shell**/**shell**.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js.gz',

'/media/ven

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **114061** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js.gz',

'/media/vendor/codemirror/mode/sieve/sieve.js',

'/media/v

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **114067** du fichier; voici le contexte :

/media/vendor/codemirror/mode/**shell**/**shell**.min.js',

'/media/vendor/codemirror/mode/**shell**/**shell**.min.js.gz',

'/media/vendor/codemirror/mode/sieve/sieve.js',

'/media/vendor/

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **151193** du fichier; voici le contexte :

lim',

'/media/vendor/codemirror/mode/sieve',

'/media/vendor/codemirror/mode/**shell**',

'/media/vendor/codemirror/mode/scheme',

'/media/vendor/codemirror/mode/sa

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **152012** du fichier; voici le contexte :

'/media/vendor/codemirror/mode/properties',

'/media/vendor/codemirror/mode/power**shell**',

'/media/vendor/codemirror/mode/pig',

'/media/vendor/codemirror/mode/php',

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_admin\src\Model\SysinfoModel.php*(21.87K)(Date dernière modif. August 27 2024 02:31:12.)*ac6c751660ff9b26d2303c6b770e26fd**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1829** du fichier; voici le contexte :
2. T\_ROOT',
3. 'extension\_dir',
4. 'error\_log',
5. 'Host',
6. 'HTTP**\_COOKIE**',
7. 'HTTP\_HOST',
8. 'HTTP\_ORIGIN',
9. 'HTTP\_REFERER',

'HTTP

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\platform\Joomla\Platform.php*(29.89K)(Date dernière modif. August 28 2024 17:47:56.)*84101925cec16b21f4f04994a6e51104**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **1588** du fichier; voici le contexte :
2. c $dbDriver = null;
3. /\*\*
4. \* Flash variables for the CLI application. We use this array since we're **hell** bent on NOT using Joomla's broken
5. \* session package.
6. \*
7. \* @var array
8. \*

\* @since 5.3.5

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\src\Controller\PushController.php*(1.73K)(Date dernière modif. August 28 2024 17:47:56.)*efd9c26c2d19ad7aaecb1317bc58a101**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **1515** du fichier; voici le contexte :
2. Name = $this->app->get('sitename');
3. $title = Text::sprintf('COM\_AKEEBABACKUP\_CONTROLPANEL\_WEBPUSH**\_HELL**O\_TITLE', $siteName);
4. $options = new NotificationOptions();

$options->body = Text::\_('COM\_AKEEBA

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **1647** du fichier; voici le contexte :

tions = new NotificationOptions();

$options->body = Text::\_('COM\_AKEEBABACKUP\_CONTROLPANEL\_WEBPUSH**\_HELL**O\_BODY');

$this->getModel()->sendNotification(

$title,

$options->toArray(),

null,

$su

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\src\Helper\Utils.php*(3.96K)(Date dernière modif. August 28 2024 17:47:56.)*4b5b96cc0c4bb2ae457eea1881394bef**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3313** du fichier; voici le contexte :
2. $returnUrl == $encoded) && (strpos($returnUrl, 'index.php') === false))
3. {
4. $possibleReturnUrl = **base64\_decode**($returnUrl);
5. if ($possibleReturnUrl !== false)
6. {
7. $returnUrl = $possibleReturnUrl;

}

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\src\Model\UpgradeHandler\MigrateSettings.php*(14.51K)(Date dernière modif. August 28 2024 17:47:56.)*1790d0efeb8c1ad9b957bb4d0df59418**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10248** du fichier; voici le contexte :
2. rocess = trim($toProcess, '\'');
3. define('AKEEBA\_MIGRATED\_SERVERKEY', $toProcess);
4. }
5. $key = @**base64\_decode**(AKEEBA\_MIGRATED\_SERVERKEY);
6. if (empty($key))
7. {
8. return;
9. }

$secSettings = Factory::getSe

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\tmpl\commontemplates\errorhandler.php*(8.21K)(Date dernière modif. August 28 2024 17:47:56.)*2ce85090fd569a36e4bdc4feed9d8526**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5722** du fichier; voici le contexte :
2. T, true)) ?></pre>
3. <h4>$\_POST</h4>
4. <pre><?= htmlentities(print\_r($\_POST, true)) ?></pre>
5. <h4>$**\_COOKIE**</h4>
6. <pre><?= htmlentities(print\_r($**\_COOKIE**, true)) ?></pre>
7. <h4>$\_REQUEST</h4>

<pre><?= html

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5768** du fichier; voici le contexte :

= htmlentities(print\_r($\_POST, true)) ?></pre>

<h4>$**\_COOKIE**</h4>

<pre><?= htmlentities(print\_r($**\_COOKIE**, true)) ?></pre>

<h4>$\_REQUEST</h4>

<pre><?= htmlentities(print\_r($\_REQUEST, true)) ?></pre>

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\tmpl\controlpanel\warnings.php*(11.37K)(Date dernière modif. August 28 2024 17:47:56.)*c902cf5dff7ecf12251b3a2d352a6b22**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **XSECURITY**Trouvé en position **4269** du fichier; voici le contexte :
2. success w-100">
3. <span class="fa fa-hammer"></span>
4. <?= Text::\_('COM\_AKEEBABACKUP\_CPANEL\_BTN\_FI**XSECURITY**') ?>
5. </button>
6. </form>
7. <?php else: ?>
8. <p>

<?= Text::\_('COM\_AKEEBABACKUP\_CPANEL\_LBL\_OUTDIR\_TR

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **XSECURITY**Trouvé en position **5410** du fichier; voici le contexte :

success w-100">

<span class="fa fa-hammer"></span>

<?= Text::\_('COM\_AKEEBABACKUP\_CPANEL\_BTN\_FI**XSECURITY**') ?>

</button>

</form>

</details>

<?php // mbstring warning ?>

<?php if(!$this->checkMbstring)

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Archiver\BaseArchiver.php*(22.35K)(Date dernière modif. August 28 2024 17:47:56.)*fffb1b8ece7aa1fc33cc9cf11b6771ce**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **9072** du fichier; voici le contexte :
2. Symlink)
3. {
4. // If we don't have gzip installed we can't compress anything
5. if (!function\_exists("**gzcompress**"))
6. {
7. return 0;
8. }
9. // Don't compress directories or symlinks

if ($isDir || $isSymlink)

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **11874** du fichier; voici le contexte :

$c\_len = $unc\_len;

$compressionMethod = 0;

// Proceed with compression

$zdata = @**gzcompress**($udata);

if ($zdata !== false)

{

// The compression succeeded

unset($udata);

$compres

×

1. D: \wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Core\Domain\Finalizer\PostProcessing.php*(9.71K)(Date dernière modif. August 28 2024 17:47:56.)*2a19f3c5171bbc87e7447714af3af9b2**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **remote file upload**Trouvé en position **1302** du fichier; voici le contexte :
2. use Exception;
3. use Akeeba\Engine\Psr\Log\LogLevel;
4. /\*\*
5. \* Performs any necessary post-processing (**remote file upload**ing) still pending.
6. \*
7. \* @since 9.3.1
8. \* @package Akeeba\Engine\Core\Domain\Finalizer

\*

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Core\Domain\Init.php*(14.55K)(Date dernière modif. August 28 2024 17:47:56.)*e2ca58f5eb5c0cd738e77bb348c1a91f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **7409** du fichier; voici le contexte :
2. Factory::getLog()->info("Current mem. usage :" . memory\_get\_usage());
3. }
4. if (function\_exists("**gzcompress**"))
5. {
6. Factory::getLog()->info("GZIP Compression : available (good)");
7. }
8. else

{

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Factory.php*(29.06K)(Date dernière modif. August 28 2024 17:47:56.)*701ec3fa2d87485779547609ec9192fa**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3843** du fichier; voici le contexte :
2. unction unserialize(string $serializedData): void
3. {
4. static::nuke();
5. $engineInfo = unserialize(**base64\_decode**($serializedData));
6. static::$root = $engineInfo['root'] ?? '';

static::$objectLi

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\FixMySQLHostname.php*(7.12K)(Date dernière modif. August 28 2024 17:47:56.)*2f8cc118542a608d0b68f42d55ad42d3**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6430** du fichier; voici le contexte :
2. be enclosed with parentheses and have \\.\ in front.
3. \*
4. \* @see https://dev.mysql.com/doc/mysql-**shell**/8.0/en/mysql-**shell**-connection-socket.html

\* @see https://www.php.net/manual/en/mysqli.quickstart

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6449** du fichier; voici le contexte :

rentheses and have \\.\ in front.

\*

\* @see https://dev.mysql.com/doc/mysql-**shell**/8.0/en/mysql-**shell**-connection-socket.html

\* @see https://www.php.net/manual/en/mysqli.quickstart.connections.php

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Complexify.php*(15.49K)(Date dernière modif. August 28 2024 17:47:56.)*cde1af865d468519c69b8bf3c3144037**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **warrior**Trouvé en position **9780** du fichier; voici le contexte :
2. hannon', 'success', 'testing', 'thunder',
3. 'thx1138', 'tiffany', 'trouble', 'twitter', 'voyager', '**warrior**', 'welcome',
4. 'william', 'winston', 'yankees', 'zxcvbnm', '11111111', '12345678', 'access14',

'b

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'hell**Trouvé en position **5995** du fichier; voici le contexte :

eam',

'david', 'dirty', 'eagle', 'enjoy', 'enter', 'frank', 'girls', 'great', 'green',

'happy', **'hell**o', 'horny', 'house', 'james', 'japan', 'jason', 'juice', 'kelly',

'kevin', 'kitty', 'lover', 'luc

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **chell**Trouvé en position **10110** du fichier; voici le contexte :

otball', 'hardcore',

'iloveyou', 'internet', 'jennifer', 'marlboro', 'maverick', 'mercedes',

'mi**chell**e', 'midnight', 'mistress', 'mountain', 'nicholas', 'password',

'princess', 'qwertyui', 'redskins'

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Encrypt.php*(27.24K)(Date dernière modif. August 28 2024 17:47:56.)*e5f4f7fd8426505cdb17be7869e79364**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10911** du fichier; voici le contexte :
2. ys
3. if (!($nBits == 128 || $nBits == 192 || $nBits == 256))
4. {
5. return '';
6. }
7. $ciphertext = **base64\_decode**($ciphertext);
8. // use AES to encrypt password (mirroring encrypt routine)

$nBytes = $nBits / 8

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\FactoryStorage.php*(7.11K)(Date dernière modif. August 28 2024 17:47:56.)*8ba83d51b1104a0f241ea5eaf9aa94ce**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6428** du fichier; voici le contexte :
2. Index = $isPHPFile ? 2 : 1;
3. switch ($parts[$encodingIndex])
4. {
5. case 'base64';
6. return **base64\_decode**($parts[$dataIndex]);
7. break;
8. case 'uuencode':

return convert\_uudecode($parts[$dataIndex]

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **uudecode**Trouvé en position **6514** du fichier; voici le contexte :

';

return base64\_decode($parts[$dataIndex]);

break;

case 'uuencode':

return convert\_**uudecode**($parts[$dataIndex]);

break;

case 'plain':

return $parts[$dataIndex];

break;

def

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **7007** du fichier; voici le contexte :

ncoding: base sixty four, handled by PHP

if (function\_exists('base64\_encode') && function\_exists('**base64\_decode**'))

{

return 'base64';

}

// Fallback: UUencoding

if (function\_exists('convert\_uuencode')

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **uudecode**Trouvé en position **7149** du fichier; voici le contexte :

}

// Fallback: UUencoding

if (function\_exists('convert\_uuencode') && function\_exists('convert\_**uudecode**'))

{

return 'uuencode';

}

// Final fallback (should NOT be necessary): plain text encodin

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\SecureSettings.php*(5.57K)(Date dernière modif. August 28 2024 17:47:56.)*91a6d8a1a580a04df26743440489abf7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2147** du fichier; voici le contexte :
2. include\_once $altFilename;
3. }
4. }
5. if (defined('AKEEBA\_SERVERKEY'))
6. {
7. $this->key = **base64\_decode**(AKEEBA\_SERVERKEY);
8. }
9. }
10. return $this->key;
11. }
12. /\*\*

\* Do the server options allow us to us

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2817** du fichier; voici le contexte :

ncode/\_decode required for encryption?

if (!function\_exists('base64\_encode') || !function\_exists('**base64\_decode**'))

{

return false;

}

// Pre-requisites met. We can encrypt and decrypt!

return true;

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5384** du fichier; voici le contexte :

pted = substr($encrypted, 12);

switch ($mode)

{

default:

case 'AES128':

$encrypted = **base64\_decode**($encrypted);

$decrypted = rtrim(Factory::getEncryption()->AESDecryptCBC($encrypted, $key), "\0"

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Statistics.php*(7.33K)(Date dernière modif. August 28 2024 17:47:56.)*22823499e280d025849a9c27a4982c08**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **brute force**Trouvé en position **3918** du fichier; voici le contexte :
2. filename))
3. {
4. $ret[] = $filename;
5. }
6. }
7. // Edge case: still running backups, we have to **brute force** the scan
8. // of existing files (multipart may be lying)
9. if ($stat['status'] == 'run')
10. {

$ba

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Transfer\Sftp.php*(14.72K)(Date dernière modif. August 28 2024 17:47:56.)*078cef39c56c9ce1837de0a003342aeb**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **11110** du fichier; voici le contexte :
2. likely to fail) raw command mode
3. else
4. {
5. $cmd = 'chmod ' . decoct($permissions) . ' ' . escape**shell**arg($fileName);
6. return @ssh2\_exec($this->connection, $cmd);
7. }
8. }
9. /\*\*

\* Create a directory

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **14665** du fichier; voici le contexte :

t($folder)

{

// First try the command for Linxu servers

$res = $this->ssh2cmd('ls -l ' . escape**shell**arg($folder));

// If an error occurred let's try the command for Windows servers

if (empty($res

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **14820** du fichier; voici le contexte :

y the command for Windows servers

if (empty($res))

{

$res = $this->ssh2cmd('CMD /C ' . escape**shell**arg($folder));

}

return $res;

}

private function ssh2cmd($command)

{

$stream = ssh2\_exec(

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\akeeba\webpush\src\Base64Url\Base64Url.php*(2.56K)(Date dernière modif. August 28 2024 17:47:56.)*4a1453661e97c93fc0b1f18b206192c7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1658** du fichier; voici le contexte :
2. ===================================================
3. \*/
4. use InvalidArgumentException;
5. use function **base64\_decode**;
6. use function base64\_encode;
7. use function rtrim;
8. use function strtr;
9. /\*\*

\* Encode and decode data

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2454** du fichier; voici le contexte :

alidArgumentException

\*

\*/

public static function decode(string $data): string

{

$decoded = **base64\_decode**(strtr($data, '-\_', '+/'), true);

if (false === $decoded)

{

throw new InvalidArgumentExceptio

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_akeebabackup\vendor\composer\ca-bundle\res\cacert.pem*(223.27K)(Date dernière modif. August 28 2024 17:47:56.)*694ccfb21bbe1b997e3e4217d0256ebb**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **45420** du fichier; voici le contexte :
2. CzAJBgNVBAYTAlVTMRAw
3. DgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxTdGFyZmllbGQg
4. VG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMuMTIwMAYDVQQDEylTdGFyZmllbGQgUm9vdCBDZXJ0aWZpY2F0ZSBB

dXRob3JpdHkgLSBHMjCCASIwDQYJK

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **46931** du fichier; voici le contexte :

CzAJBgNV

BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxT

dGFyZmllbGQgVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMuMTswOQYDVQQDEzJTdGFyZmllbGQgU2VydmljZXMg

Um9vdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgLSBHM

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **N5c3Rlb**Trouvé en position **56243** du fichier; voici le contexte :

0Q0EyMB4XDTA5MDUyOTA1MDAzOVoXDTI5MDUyOTA1MDAzOVowXTELMAkGA1UEBhMC

SlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">N5c3Rlb**XMgQ08uLExURC4xJzAlBgNVBAsTHlNlY3Vy

aXR5IENvbW11bmljYXRpb24gUm9vdENBMjCCASIwDQYJKoZIhvcNAQEBBQADggEP

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **109420** du fichier; voici le contexte :

gAwIBAgIQIdbQSk8lD8kyN/yqXhKN6TANBgkqhkiG9w0BAQ0FADCBgDELMAkGA1UE

BhMCUEwxIjAgBgNVBAoTGVVuaXpldG8gVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzIFMuQS4xJzAlBgNVBAsTHkNlcnR1

bSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEkMCIGA1UEAxMbQ2VydHVtIFRyd

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **N5c3Rlb**Trouvé en position **203762** du fichier; voici le contexte :

0Q0ExMB4XDTE2MDYxNjA1MTUyOFoXDTM4MDExODA1MTUyOFowYTEL

MAkGA1UEBhMCSlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">N5c3Rlb**XMgQ08uLExURC4xKzApBgNV

BAMTIlNlY3VyaXR5IENvbW11bmljYXRpb24gRUNDIFJvb3RDQTEwdjAQBgcqhkjOPQIBBgUrgQQA

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **216274** du fichier; voici le contexte :

DQSBHMzAeFw0yMTA1MjAwMjEwMTlaFw00NjA1MTkwMjEw

MTlaMFoxCzAJBgNVBAYTAkNOMSUwIwYDVQQKDBxUcnVzdEFzaWEgVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMu

MSQwIgYDVQQDDBtUcnVzdEFzaWEgR2xvYmFsIFJvb3QgQ0EgRzMwggIiMA0GCSqGSIb3DQEBAQUA

A4IC

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **218339** du fichier; voici le contexte :

DQSBHNDAeFw0yMTA1MjAwMjEwMjJaFw00NjA1MTkwMjEwMjJa

MFoxCzAJBgNVBAYTAkNOMSUwIwYDVQQKDBxUcnVzdEFzaWEgVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMuMSQw

IgYDVQQDDBtUcnVzdEFzaWEgR2xvYmFsIFJvb3QgQ0EgRzQwdjAQBgcqhkjOPQIBBgUrgQQAIgNi

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_config\src\Controller\ComponentController.php*(6.81K)(Date dernière modif. August 27 2024 02:31:12.)*3ef0f43132db4a0cb5d84ed67d72530c**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5737** du fichier; voici le contexte :
2. .php?option=' . $option;
3. if (!empty($returnUri)) {
4. $redirect = **base64\_decode**($returnUri);
5. }

// Don't redirect to an external URL.

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6716** du fichier; voici le contexte :

rect = 'index.php?option=' . $component;

if (!empty($returnUri)) {

$redirect = **base64\_decode**($returnUri);

}

// Don't redirect to an external URL.

if (!Uri::isInternal(

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_config\tmpl\application\default\_cookie.php*(628.00B)(Date dernière modif. August 27 2024 02:31:12.)*c71784002f70482d893a3f24e1a6569f**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **449** du fichier; voici le contexte :
2. Component\Config\Administrator\View\Application\HtmlView $this \*/
3. $this->name = Text::\_('COM\_CONFIG**\_COOKIE**\_SETTINGS');
4. $this->description = '';
5. $this->fieldsname = 'cookie';

$this->formclass = 'options-form

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_icagenda\CHANGELOG.php*(398.89K)(Date dernière modif. August 28 2024 17:48:10.)*9b44567eaab6d5f826257341ceadcf38**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **SQL injection**Trouvé en position **163961** du fichier; voici le contexte :
2. .0 through 3.7.13
3. 1 Description: The lack of type casting of a variable in SQL statement leads to a **SQL injection** vulnerability in the events list view.

+ Added : Search in custom fields value with the frontend gl

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_icagenda\src\Utilities\Manager\Manager.php*(7.97K)(Date dernière modif. August 28 2024 17:48:12.)*7fb4419486f536b0ad4ad5f0615f9e14**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **6684** du fichier; voici le contexte :
2. ias ?: $item->username;
3. $approvedbodycontent = Text::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $creator) . ',<br /><br />';

$approvedbodycontent.= Text::sprintf('COM\_ICAGENDA\_APPROVED\_USER

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_icagenda\utilities\manager\manager.php*(6.70K)(Date dernière modif. August 28 2024 17:48:12.)*5145b3754e8007c0bc46f24525c5f3a0**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **5793** du fichier; voici le contexte :
2. as ?: $item->username;
3. $approvedbodycontent = JText::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $creator) . ',<br /><br />';

$approvedbodycontent.= JText::sprintf('COM\_ICAGENDA\_APPROVED\_USE

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_installer\src\Controller\InstallController.php*(3.33K)(Date dernière modif. August 27 2024 02:31:12.)*15b68c880abc22dfc4b71b56c745d053**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1633** du fichier; voici le contexte :
2. ->input->getBase64('return');
3. if (!$redirect\_url && $return) {
4. $redirect\_url = **base64\_decode**($return);
5. }
6. // Don't redirect to an external URL.

if ($redirect\_url && !Ur

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_jce\helpers\encrypt\aes.php*(22.04K)(Date dernière modif. August 31 2024 15:58:02.)*0fe3e6c4edd58f48c03dea8497a86012**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14018** du fichier; voici le contexte :
2. = 256)) {
3. return '';
4. } // standard allows 128/192/256 bit keys
5. $ciphertext = **base64\_decode**($ciphertext);
6. // use AES to encrypt password (mirroring encrypt routine)

$nBytes = $nB

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_jce\helpers\encrypt.php*(4.13K)(Date dernière modif. August 31 2024 15:58:02.)*7181bf8e9c3b05560e8b832769629075**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1454** du fichier; voici le contexte :
2. ERVERKEY')) {
3. // return key as string
4. if ($legacy) {
5. $key = **base64\_decode**(WF\_SERVERKEY);
6. return $key;
7. }
8. try {

$keyAs

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3205** du fichier; voici le contexte :

switch ($mode) {

case '###AES128###':

$encrypted = **base64\_decode**($encrypted);

$decrypted = @WFUtilEncrypt::AESDecryptCBC($encrypted, $key, 128);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3891** du fichier; voici le contexte :

encrypted = substr($encrypted, 12);

// base64decode

$decoded = **base64\_decode**($encrypted);

try {

$decrypted = Crypto::decrypt($decoded, $key);

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_jce\vendor\Defuse\Crypto\Crypto.php*(13.99K)(Date dernière modif. August 31 2024 15:58:02.)*77bfdbf16d0f59a615ec9c702c6e9eaf**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **1070** du fichier; voici le contexte :
2. \* Encrypts a string with a password, using a slow key derivation function
3. \* to make password **cracking** more expensive.
4. \*
5. \* @param string $plaintext
6. \* @param string $password

\* @param

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **3258** du fichier; voici le contexte :

iphertext to a string with a password, using a slow key

\* derivation function to make password **cracking** more expensive.

\*

\* @param string $ciphertext

\* @param string $password

\* @para

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_jce\vendor\Defuse\Crypto\File.php*(24.92K)(Date dernière modif. August 31 2024 15:58:02.)*1a0b019a98d21149a6c4c691e5c58969**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **742** du fichier; voici le contexte :
2. \* Encrypts a file with a password, using a slow key derivation function to
3. \* make password **cracking** more expensive.
4. \*
5. \* @param string $inputFilename

\* @param string $outputFilename

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **1967** du fichier; voici le contexte :

\* Decrypts a file with a password, using a slow key derivation function to

\* make password **cracking** more expensive.

\*

\* @param string $inputFilename

\* @param string $outputFilename

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **3310** du fichier; voici le contexte :

e handle into another with a

\* password, using a slow key derivation function to make password **cracking**

\* more expensive.

\*

\* @param resource $inputHandle

\* @param resource $outputHan

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **4684** du fichier; voici le contexte :

resource into another with a password, using

\* a slow key derivation function to make password **cracking** more expensive.

\*

\* @param resource $inputHandle

\* @param resource $outputHandle

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_joomlaupdate\extract.php*(60.13K)(Date dernière modif. August 27 2024 02:31:12.)*ef6710b62dfb745edc7c3f4d1831feb9**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **brute force**Trouvé en position **54414** du fichier; voici le contexte :
2. that it's stale and someone forgot to
3. \* remove it from the server.
4. \*
5. \* This prevents **brute force** attacks against the randomly generated password. Even a simple 8 character simple

\* alphanum (

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **brute force**Trouvé en position **54797** du fichier; voici le contexte :

requiring going over just 1% of

\* the search space it'd still take over 282 million seconds to **brute force** it. Our limit is more than 4 orders

\* of magnitude lower than this best practical case scenari

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **12263** du fichier; voici le contexte :

alized = serialize($clone);

return (\function\_exists('base64\_encode') && \function\_exists('**base64\_decode**')) ? base64\_encode($serialized) : $serialized;

}

/\*\*

\* Restores a serialised instance

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **12881** du fichier; voici le contexte :

string $serialised): ?self

{

if (\function\_exists('base64\_encode') && \function\_exists('**base64\_decode**')) {

$serialised = **base64\_decode**($serialised);

}

$instance = @unserial

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **12926** du fichier; voici le contexte :

\function\_exists('base64\_encode') && \function\_exists('**base64\_decode**')) {

$serialised = **base64\_decode**($serialised);

}

$instance = @unserialize($serialised, [

'allowed\_c

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_login\src\Model\LoginModel.php*(6.27K)(Date dernière modif. August 27 2024 02:31:12.)*eb35ebe703f6a2738857127529ed1a68**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1472** du fichier; voici le contexte :
2. e request first.
3. if ($return = $input->get('return', '', 'BASE64')) {
4. $return = **base64\_decode**($return);
5. if (!Uri::isInternal($return)) {
6. $return = '';

}

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_mails\src\Controller\TemplateController.php*(10.64K)(Date dernière modif. August 27 2024 02:31:12.)*f29e97b2f6e12386eb7edcd3b9bc97c7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10486** du fichier; voici le contexte :
2. s->input->get('return', null, 'base64');
3. if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {
4. $url = **base64\_decode**($return);

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10540** du fichier; voici le contexte :

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this-

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_media\src\Controller\ApiController.php*(13.24K)(Date dernière modif. August 27 2024 02:31:12.)*62a10779bd113b2edebb64915b03a291**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6991** du fichier; voici le contexte :
2. = $this->input->json;
3. $name = $content->getString('name');
4. $mediaContent = **base64\_decode**($content->get('content', '', 'raw'));

$override = $content->get('override', false);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9386** du fichier; voici le contexte :

content = $this->input->json;

$name = basename($path);

$mediaContent = **base64\_decode**($content->get('content', '', 'raw'));

$newPath = $content->getString('newPath', null);

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_menus\src\Controller\ItemController.php*(19.96K)(Date dernière modif. August 27 2024 02:31:12.)*9734193fdd41bf24f925ab3b84bd4c37**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17573** du fichier; voici le contexte :
2. 'array');
3. // Get the type.
4. $type = $data['type'];
5. $type = json\_decode(**base64\_decode**($type));
6. $title = $type->title ?? null;
7. $recordId = $type->id ?? 0;

$sp

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_modules\src\Controller\ModuleController.php*(11.36K)(Date dernière modif. August 27 2024 02:31:12.)*d94ada44e476ddeb7aed99c224f62869**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2594** du fichier; voici le contexte :
2. ', null);
3. if ($return = $this->input->get('return', '', 'BASE64')) {
4. $return = **base64\_decode**($return);
5. // Don't redirect to an external URL.

if (!Uri::isInternal($retu

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_phocagallery\controllers\phocagalleryt.php*(6.09K)(Date dernière modif. July 18 2024 18:51:34.)*21c61385c1fb194c7cb162fa6145f66d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1247** du fichier; voici le contexte :
2. jexit(Text::\_('JINVALID\_TOKEN'));
3. $fileid = $this->input->get('fileid');
4. $fileid = urldecode(**base64\_decode**($fileid));
5. $model = $this->getModel();
6. echo $model->getFileContent($fileid);

Factory::getApp

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_phocagallery\libraries\phocagallery\file\fileupload.php*(30.77K)(Date dernière modif. July 18 2024 18:51:34.)*27292920da0888054200d0bf0da951d3**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15191** du fichier; voici le contexte :
2. /\*if ($return) {
3. $app->enqueueMessage( $errUploadMsg, 'error');
4. $app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);
5. exit;
6. } else {

$app->enqueueMessage( $errUploadMs

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15527** du fichier; voici le contexte :

$app->enqueueMessage( $errUploadMsg, 'error');

if ($frontEnd > 0) {

$app->redirect(**base64\_decode**($return));

} else {

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15589** du fichier; voici le contexte :

ontEnd > 0) {

$app->redirect(**base64\_decode**($return));

} else {

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

}

exit;

} else {

$app->enqueueMessage( $err

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15950** du fichier; voici le contexte :

pp->enqueueMessage( Text::\_('COM\_PHOCAGALLERY\_FILE\_ALREADY\_EXISTS'), 'error');

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

$app->enqueueMessage(Text::\_('COM\_

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **16377** du fichier; voici le contexte :

eueMessage( Text::\_('COM\_PHOCAGALLERY\_ERROR\_UNABLE\_TO\_UPLOAD\_FILE'), 'error');

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

$app->enqueueMessage( Text::\_('COM

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **16803** du fichier; voici le contexte :

$app->enqueueMessage( Text::\_('COM\_PHOCAGALLERY\_SUCCESS\_FILE\_UPLOAD'));

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

$app->enqueueMessage( Text::\_('COM

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17169** du fichier; voici le contexte :

R\_UNABLE\_TO\_UPLOAD\_FILE');

if ($return) {

$app->enqueueMessage( $msg);

$app->redirect(**base64\_decode**($return).'&folder='.$folderUrl);

exit;

} else {

switch ($viewBack) {

case 'phoc

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_privacy\src\Controller\RequestController.php*(11.66K)(Date dernière modif. August 27 2024 02:31:12.)*277329b675f6a115f56b6695353512a1**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3828** du fichier; voici le contexte :
2. n = $this->input->get('return', null, 'base64');
3. if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {
4. $url = **base64\_decode**($return);
5. }

// Redirect to the list

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3874** du fichier; voici le contexte :

);

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this->setRedirect(Route::\_($u

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4942** du fichier; voici le contexte :

n = $this->input->get('return', null, 'base64');

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4988** du fichier; voici le contexte :

);

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this->setRedirect(Route::\_($u

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **8276** du fichier; voici le contexte :

n = $this->input->get('return', null, 'base64');

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **8322** du fichier; voici le contexte :

);

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this->setRedirect(Route::\_($u

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9611** du fichier; voici le contexte :

n = $this->input->get('return', null, 'base64');

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9657** du fichier; voici le contexte :

);

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this->setRedirect(Route::\_($u

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_privacy\src\Model\CapabilitiesModel.php*(4.33K)(Date dernière modif. August 27 2024 02:31:12.)*7ec6de98f806677096e1ad7cec447c59**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1860** du fichier; voici le contexte :
2. CORE\_CAPABILITIES') => [
3. Text::\_('COM\_PRIVACY\_CORE\_CAPABILITY\_SESSION\_IP\_ADDRESS\_AND**\_COOKIE**'),

Text::sprintf('COM\_PRIVACY\_CORE\_CAPABILITY\_LOGGING\_IP\_ADDRESS', $app->get('log\_p

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_templates\src\Controller\TemplateController.php*(36.97K)(Date dernière modif. August 27 2024 02:31:12.)*e16a38ebba1ea2eab3ac28a8f0cd9171**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9245** du fichier; voici le contexte :
2. ring) $this->input->getCmd('file', '');
3. $explodeArray = explode(':', str\_replace('//', '/', **base64\_decode**($fileName)));
4. // Access check.
5. if (!$this->allowEdit()) {

$this->setMe

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **13374** du fichier; voici le contexte :

\_DEFINED\_TAGS,

InputFilter::ONLY\_BLOCK\_DEFINED\_ATTRIBUTES

)

->clean(**base64\_decode**($this->input->getBase64('folder', '')), 'path');

$id = (int) $this->input->get('id',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14644** du fichier; voici le contexte :

'JLIB\_APPLICATION\_ERROR\_SAVE\_NOT\_PERMITTED'), 'error');

return;

}

if (**base64\_decode**(urldecode($file)) == '/index.php') {

$this->setMessage(Text::\_('COM\_TEMPLATES\_ERROR\_IND

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15002** du fichier; voici le contexte :

put->getInt('isMedia', 0);

$this->setRedirect(Route::\_($url, false));

} elseif (**base64\_decode**(urldecode($file)) == '/joomla.asset.json') {

$this->setMessage(Text::\_('COM\_TEMPLATES\_E

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **16807** du fichier; voici le contexte :

\_DEFINED\_TAGS,

InputFilter::ONLY\_BLOCK\_DEFINED\_ATTRIBUTES

)

->clean(**base64\_decode**($this->input->getBase64('address', '')), 'path');

$type = (string) $this->input->get('t

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **19318** du fichier; voici le contexte :

\_DEFINED\_TAGS,

InputFilter::ONLY\_BLOCK\_DEFINED\_ATTRIBUTES

)

->clean(**base64\_decode**($this->input->getBase64('address', '')), 'path');

// Access check.

if (!$this->all

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **21064** du fichier; voici le contexte :

\_DEFINED\_TAGS,

InputFilter::ONLY\_BLOCK\_DEFINED\_ATTRIBUTES

)

->clean(**base64\_decode**($this->input->getBase64('address', '')), 'path');

// Access check.

if (!$this->all

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **23090** du fichier; voici le contexte :

\_DEFINED\_TAGS,

InputFilter::ONLY\_BLOCK\_DEFINED\_ATTRIBUTES

)

->clean(**base64\_decode**($this->input->getBase64('address', '')), 'path');

// Access check.

if (!$this->all

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **23801** du fichier; voici le contexte :

$this->setMessage(Text::\_('COM\_TEMPLATES\_FOLDER\_DELETE\_SUCCESS'));

if (stristr(**base64\_decode**($file), $location) != false) {

$file = base64\_encode('home');

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **25166** du fichier; voici le contexte :

'JLIB\_APPLICATION\_ERROR\_SAVE\_NOT\_PERMITTED'), 'error');

return;

}

if (**base64\_decode**(urldecode($file)) == '/index.php') {

$this->setMessage(Text::\_('COM\_TEMPLATES\_ERROR\_REN

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **25498** du fichier; voici le contexte :

. '&isMedia=' . $isMedia;

$this->setRedirect(Route::\_($url, false));

} elseif (**base64\_decode**(urldecode($file)) == '/joomla.asset.json') {

$this->setMessage(Text::\_('COM\_TEMPLATES\_E

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **30639** du fichier; voici le contexte :

\_DEFINED\_TAGS,

InputFilter::ONLY\_BLOCK\_DEFINED\_ATTRIBUTES

)

->clean(**base64\_decode**($this->input->getBase64('address', '')), 'path');

/\*\* @var \Joomla\Component\Templates\Adm

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_templates\src\Model\TemplateModel.php*(69.24K)(Date dernière modif. August 27 2024 02:31:12.)*cfc09def59abacc4124a21646e700890**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6198** du fichier; voici le contexte :
2. ($pk->client\_id);
3. $path = Path::clean($client->path . '/templates/' . $pk->template . **base64\_decode**($pk->hash\_id));
4. if (file\_exists($path)) {

$results[] = $pk;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **29535** du fichier; voici le contexte :

>template) {

$input = Factory::getApplication()->getInput();

$fileName = **base64\_decode**($input->get('file'));

$fileName = str\_replace('//', '/', $fileName);

$isMed

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **31753** du fichier; voici le contexte :

return false;

}

$app = Factory::getApplication();

$fileName = **base64\_decode**($app->getInput()->get('file'));

$isMedia = $app->getInput()->getInt('isMedia', 0);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **43827** du fichier; voici le contexte :

$app = Factory::getApplication();

$filePath = $this->getBasePath() . urldecode(**base64\_decode**($file));

$return = File::delete($filePath);

if (!$return) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **49184** du fichier; voici le contexte :

ry::getApplication();

$path = $this->getBasePath();

$fileName = **base64\_decode**($file);

$explodeArray = explode('.', $fileName);

$type = end($explo

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **50228** du fichier; voici le contexte :

($this->getTemplate()) {

$app = Factory::getApplication();

$fileName = **base64\_decode**($app->getInput()->get('file'));

$path = $this->getBasePath();

$uri = U

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **51577** du fichier; voici le contexte :

{

$app = Factory::getApplication();

$path = $this->getBasePath() . **base64\_decode**($file);

try {

$image = new Image($path);

$propert

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **53054** du fichier; voici le contexte :

late()) {

$app = Factory::getApplication();

$path = $this->getBasePath() . **base64\_decode**($file);

try {

$image = new Image($path);

$propert

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **55347** du fichier; voici le contexte :

$client = ApplicationHelper::getClientInfo($template->client\_id);

$relPath = **base64\_decode**($app->getInput()->get('file'));

$explodeArray = explode('/', $relPath);

$fi

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **55544** du fichier; voici le contexte :

$fileName = end($explodeArray);

$path = $this->getBasePath() . **base64\_decode**($app->getInput()->get('file'));

if (stristr($client->path, 'administrator') == false)

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **56814** du fichier; voici le contexte :

getTemplate()) {

$app = Factory::getApplication();

$relPath = **base64\_decode**($file);

$explodeArray = explode('.', $relPath);

$ext = end($explod

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **57805** du fichier; voici le contexte :

late()) {

$app = Factory::getApplication();

$path = $this->getBasePath() . **base64\_decode**($app->getInput()->get('file'));

if (file\_exists(Path::clean($path))) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **59016** du fichier; voici le contexte :

getTemplate()) {

$app = Factory::getApplication();

$relPath = **base64\_decode**($file);

$explodeArray = explode('/', $relPath);

$fileName = end($explod

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **59189** du fichier; voici le contexte :

$fileName = end($explodeArray);

$path = $this->getBasePath() . **base64\_decode**($file);

if (file\_exists(Path::clean($path . '/' . $fileName))) {

$zip

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_templates\src\View\Template\HtmlView.php*(12.22K)(Date dernière modif. August 27 2024 02:31:12.)*fda7f380173a473bf38daedc7289971f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3149** du fichier; voici le contexte :
2. = $app->getInput()->get('file', '');
3. $this->fileName = InputFilter::getInstance()->clean(**base64\_decode**($this->file), 'string');
4. $explodeArray = explode('.', $this->fileName);

$ext

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_templates\tmpl\template\default.php*(26.27K)(Date dernière modif. August 27 2024 02:31:12.)*5ad15162dec03e4e4ac11fbd91d6c881**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2228** du fichier; voici le contexte :

ient\_id === 0 ? 'site' : 'administrator') . '/' . $this->template->element . str\_replace('//', '/', **base64\_decode**($this->file)) : '/' . ((int) $this->template->client\_id === 0 ? '' : 'administrator/') . 'templates

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2396** du fichier; voici le contexte :

d === 0 ? '' : 'administrator/') . 'templates/' . $this->template->element . str\_replace('//', '/', **base64\_decode**($this->file))), $this->template->element); ?></p>

<p class="lead path hidden"><?php

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_templates\tmpl\template\default\_updated\_files.php*(5.18K)(Date dernière modif. August 27 2024 02:31:12.)*07f39341dbe1bb8aee5c31b1fec56613**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3822** du fichier; voici le contexte :
2. ion\_id . '&file=' . $value->hash\_id); ?>" title="<?php echo Text::\_('JACTION\_EDIT'); ?>"><?php echo **base64\_decode**($value->hash\_id); ?></a>
3. </td>

<td>

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\Controller\MailController.php*(1.61K)(Date dernière modif. August 27 2024 02:31:12.)*b4c2e2a33964bd9927ef33b33299d58d**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mass mailer**Trouvé en position **738** du fichier; voici le contexte :
2. \*
3. \* @since 1.6
4. \*/
5. public function send()
6. {
7. // Redirect to admin index if **mass mailer** disabled in conf
8. if ($this->app->get('massmailoff', 0) == 1) {

$this->app->redi

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\Controller\MethodController.php*(15.73K)(Date dernière modif. August 27 2024 02:31:12.)*4ec7eddd283413d875ed3b9f3a720d88**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **7082** du fichier; voici le contexte :
2. urnURL = $this->input->getBase64('returnurl');
3. if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {
4. $redirectUrl .= '&returnurl=' . $returnURL;
5. }

$this->s

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **8971** du fichier; voici le contexte :

eturnURL = $this->input->getBase64('returnurl');

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

$this->setRedirect

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9020** du fichier; voici le contexte :

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

$this->setRedirect($url, $message, $type);

}

/\*\*

\* Sa

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10000** du fichier; voici le contexte :

eturnURL = $this->input->getBase64('returnurl');

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

// The record must

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10049** du fichier; voici le contexte :

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

// The record must either be new (ID zero) or exist

$id

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\Controller\MethodsController.php*(7.28K)(Date dernière modif. August 27 2024 02:31:12.)*e8846ce041fd8050904d08a3e45a6132**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3678** du fichier; voici le contexte :
2. eturnURL = $this->input->getBase64('returnurl');
3. if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {
4. $url = **base64\_decode**($returnURL);
5. }

$this->setRedirect

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3727** du fichier; voici le contexte :

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

$this->setRedirect($url, $message, $type);

}

/\*\*

\* Li

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6941** du fichier; voici le contexte :

eturnURL = $this->input->getBase64('returnurl');

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

$this->setRedirect

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6990** du fichier; voici le contexte :

if (!empty($returnURL) && Uri::isInternal(**base64\_decode**($returnURL))) {

$url = **base64\_decode**($returnURL);

}

$this->setRedirect($url);

}

/\*\*

\* Assert that there i

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\Controller\UserController.php*(4.55K)(Date dernière modif. August 27 2024 02:31:12.)*383269901c0591c7ede1ea88a42ff267**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2264** du fichier; voici le contexte :
2. cancel();
3. if ($return = $this->input->get('return', '', 'BASE64')) {
4. $return = **base64\_decode**($return);
5. // Don't redirect to an external URL.

if (!Uri::isInternal($retu

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3197** du fichier; voici le contexte :

f ($task === 'save' && $return = $this->input->get('return', '', 'BASE64')) {

$return = **base64\_decode**($return);

// Don't redirect to an external URL.

if (!Uri::isInternal($retu

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\Model\UsersModel.php*(20.07K)(Date dernière modif. August 27 2024 02:31:12.)*ef386a70e8cc6b7c6655ab7ab9d7fd05**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2880** du fichier; voici le contexte :
2. t', 'cmd')) {
3. $this->context .= '.' . $layout;
4. }
5. $groups = json\_decode(**base64\_decode**($input->get('groups', '', 'BASE64')));
6. if (isset($groups)) {

$groups = ArrayHe

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3114** du fichier; voici le contexte :

ps);

}

$this->setState('filter.groups', $groups);

$excluded = json\_decode(**base64\_decode**($input->get('excluded', '', 'BASE64')));

if (isset($excluded)) {

$excluded = A

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\View\Mail\HtmlView.php*(2.14K)(Date dernière modif. August 27 2024 02:31:12.)*8b6921a787da216e553c24e163880796**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **mass mailer**Trouvé en position **1109** du fichier; voici le contexte :
2. eption
3. \*/
4. public function display($tpl = null)
5. {
6. // Redirect to admin index if **mass mailer** disabled in conf
7. if (Factory::getApplication()->get('massmailoff', 0) == 1) {

F

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\src\View\Method\HtmlView.php*(6.46K)(Date dernière modif. August 27 2024 02:31:12.)*a21340a36dc218398de1ef2f566dee2b**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4465** du fichier; voici le contexte :
2. }
3. $this->title = '';
4. }
5. $returnUrl = empty($this->returnURL) ? '' : **base64\_decode**($this->returnURL);
6. $returnUrl = ($returnUrl && Uri::isInternal($returnUrl))

? $

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\tmpl\method\backupcodes.php*(2.64K)(Date dernière modif. August 27 2024 02:31:12.)*8f86ac224b340fbf6ce467643716d6bd**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **714** du fichier; voici le contexte :
2. splay&user\_id=' . $this->user->id);
3. if (!empty($this->returnURL)) {
4. $cancelURL = $this->escape(**base64\_decode**($this->returnURL));
5. }
6. if ($this->record->method != 'backupcodes') {

throw new RuntimeException

×

1. D:\wamp64\www\randophil.J5\administrator\components\com\_users\tmpl\method\edit.php*(7.92K)(Date dernière modif. August 27 2024 02:31:12.)*ab36a152bd1ced6559b9037e1c4a2f76**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **673** du fichier; voici le contexte :
2. splay&user\_id=' . $this->user->id);
3. if (!empty($this->returnURL)) {
4. $cancelURL = $this->escape(**base64\_decode**($this->returnURL));
5. }
6. $recordId = (int) $this->record->id ?? 0;

$method = $this->record-

×

1. D:\wamp64\www\randophil.J5\api\components\com\_media\src\Controller\MediaController.php*(11.60K)(Date dernière modif. August 27 2024 02:31:12.)*2022e18b8bb53e5e51c2c4aec6fbcc31**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9490** du fichier; voici le contexte :
2. e]);
3. $json = $this->input->json;
4. // Decode content, if any
5. if ($content = **base64\_decode**($json->get('content', '', 'raw'))) {
6. $this->checkContent();
7. }

// If th

×

1. D:\wamp64\www\randophil.J5\components\com\_config\src\Controller\ModulesController.php*(5.54K)(Date dernière modif. August 27 2024 02:31:12.)*b0bec6893960947828489646ad8bc00f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5441** du fichier; voici le contexte :
2. {
3. if ($return = $this->input->post->get('return', '', 'BASE64')) {
4. $return = **base64\_decode**(urldecode($return));
5. // Only redirect to if it is an internal URL

if (Uri:

×

1. D:\wamp64\www\randophil.J5\components\com\_contact\src\Controller\ContactController.php*(14.93K)(Date dernière modif. August 27 2024 02:31:12.)*26f4a2af29b3354aa7cd24eb9c8feda9**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15174** du fichier; voici le contexte :
2. turn = $this->input->get('return', null, 'base64');
3. if (empty($return) || !Uri::isInternal(**base64\_decode**($return))) {
4. return Uri::base();
5. }

return **base64\_decode**($return);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **15259** du fichier; voici le contexte :

ri::isInternal(**base64\_decode**($return))) {

return Uri::base();

}

return **base64\_decode**($return);

}

}

×

1. D:\wamp64\www\randophil.J5\components\com\_contact\src\Model\FormModel.php*(6.44K)(Date dernière modif. August 27 2024 02:31:12.)*0bc2b9b064a431a1a94fa0c8991c9e8a**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5183** du fichier; voici le contexte :
2. '));
3. $return = $input->get('return', '', 'base64');
4. $this->setState('return\_page', **base64\_decode**($return));
5. // Load the parameters.
6. $params = $app->getParams();

$this->set

×

1. D:\wamp64\www\randophil.J5\components\com\_content\src\Controller\ArticleController.php*(12.17K)(Date dernière modif. August 27 2024 02:31:12.)*7f06b681ce260c1822d5e03989137093**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9150** du fichier; voici le contexte :
2. turn = $this->input->get('return', null, 'base64');
3. if (empty($return) || !Uri::isInternal(**base64\_decode**($return))) {
4. return Uri::base();
5. }

return **base64\_decode**($return);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9235** du fichier; voici le contexte :

ri::isInternal(**base64\_decode**($return))) {

return Uri::base();

}

return **base64\_decode**($return);

}

/\*\*

\* Method to save a record.

\*

\* @param string $key Th

×

1. D:\wamp64\www\randophil.J5\components\com\_content\src\Model\FormModel.php*(10.73K)(Date dernière modif. August 27 2024 02:31:12.)*9c5233e0aabe38cdd205b1d4cf024647**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1920** du fichier; voici le contexte :
2. d));
3. $return = $input->get('return', '', 'base64');
4. $this->setState('return\_page', **base64\_decode**($return));
5. $this->setState('layout', $input->getString('layout'));
6. }
7. /\*\*

\* M

×

1. D:\wamp64\www\randophil.J5\components\com\_icagenda\models\submit.php*(40.74K)(Date dernière modif. August 28 2024 17:48:10.)*de2910065b023642da9a7cdb15c3d8dc**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **31078** du fichier; voici le contexte :
2. f User Notification Email
3. $adminbodycontent = JText::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $username) . ',<br /><br />';
4. if ($type == 'approval')
5. {

$adminbodycontent.= JText::\_

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **34599** du fichier; voici le contexte :

;

// Set Body of Notification Email

$user\_submit\_body = JText::sprintf('COM\_ICAGENDA\_USER\_EMAIL**\_HELL**O', $username) . ',<br /><br />';

$user\_submit\_body.= JText::sprintf('COM\_ICAGENDA\_EVENT\_SUBMISSIO

×

1. D:\wamp64\www\randophil.J5\components\com\_icagenda\src\Model\SubmitModel.php*(41.78K)(Date dernière modif. August 28 2024 17:48:10.)*209ec431da8303e7f1b123687cde458d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **31148** du fichier; voici le contexte :
2. of User Notification Email
3. $adminbodycontent = Text::sprintf('COM\_ICAGENDA\_SUBMISSION\_ADMIN\_EMAIL**\_HELL**O', $username) . ',<br /><br />';
4. if ($type == 'approval') {

$adminbodycontent.= Text::\_('CO

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **\_HELL**Trouvé en position **35128** du fichier; voici le contexte :

);

// Set Body of Notification Email

$user\_submit\_body = Text::sprintf('COM\_ICAGENDA\_USER\_EMAIL**\_HELL**O', $username) . ',<br /><br />';

$user\_submit\_body.= Text::sprintf('COM\_ICAGENDA\_EVENT\_SUBMISSION

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\libraries\classes\editor.php*(45.22K)(Date dernière modif. August 31 2024 15:58:02.)*4d9552ff967310e74f9f11586fba09fe**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **12344** du fichier; voici le contexte :
2. lode(',', $stylesheets);
3. // use cookies to store state
4. $settings['use\_state**\_cookie**s'] = (bool) $wf->getParam('editor.use**\_cookie**s', 1);
5. // Set active tab

$set

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **12389** du fichier; voici le contexte :

cookies to store state

$settings['use\_state**\_cookie**s'] = (bool) $wf->getParam('editor.use**\_cookie**s', 1);

// Set active tab

$settings['active\_tab'] = 'wf-editor-' . $wf->get

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\libraries\classes\encrypt.php*(22.04K)(Date dernière modif. August 31 2024 15:58:02.)*0fe3e6c4edd58f48c03dea8497a86012**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14018** du fichier; voici le contexte :
2. = 256)) {
3. return '';
4. } // standard allows 128/192/256 bit keys
5. $ciphertext = **base64\_decode**($ciphertext);
6. // use AES to encrypt password (mirroring encrypt routine)

$nBytes = $nB

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\libraries\classes\manager\base.php*(8.81K)(Date dernière modif. August 31 2024 15:58:02.)*937df2eeda429d16c920b6600fd052e4**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **8718** du fichier; voici le contexte :
2. filebrowser\_position', $this->getParam('editor.browser\_position', 'bottom')),
3. 'use\_state**\_cookie**s' => $this->getParam('editor.use**\_cookie**s', true),

'search\_depth' => $this->getParam('ed

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **8758** du fichier; voici le contexte :

editor.browser\_position', 'bottom')),

'use\_state**\_cookie**s' => $this->getParam('editor.use**\_cookie**s', true),

'search\_depth' => $this->getParam('editor.filebrowser\_search\_depth', 3),

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\libraries\classes\mobile.php*(86.72K)(Date dernière modif. October 04 2023 16:06:24.)*6260e844bd234c942dd99b1d07c6c8ba**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **ia\_archiver**Trouvé en position **56614** du fichier; voici le contexte :

L|s~amp-validator|AdsBot-Google|Google Keyword Suggestion|Facebot|YandexBot|YandexMobileBot|bingbot|**ia\_archiver**|AhrefsBot|Ezooms|GSLFbot|WBSearchBot|Twitterbot|TweetmemeBot|Twikle|PaperLiBot|Wotbox|UnwindFetchor

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\libraries\classes\vendor\cssmin\src\Colors.php*(5.36K)(Date dernière modif. August 31 2024 15:58:02.)*9504199f1ce1ba7d7d7dfba451246fa7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **5078** du fichier; voici le contexte :
2. b4513',
3. 'sandybrown' => '#f4a460',
4. 'seagreen' => '#2e8b57',
5. 'sea**shell**' => '#fff5ee',
6. 'slateblue' => '#6a5acd',

'slategray' => '#708090',

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\plugins\spellchecker\config.php*(1.81K)(Date dernière modif. August 31 2024 15:58:02.)*b56012fca4671635c713eaae185c1743**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **826** du fichier; voici le contexte :
2. $engine = 'browser';
3. break;
4. case 'pspell':
5. case 'pspell**shell**':

$languages = (array) $wf->getParam('spellchecker.languages', 'English=en', '');

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **970** du fichier; voici le contexte :

$wf->getParam('spellchecker.languages', 'English=en', '');

if ($engine === 'pspell**shell**') {

$engine = 'pspell';

}

if (!function\_exists

×

1. D:\wamp64\www\randophil.J5\components\com\_jce\editor\plugins\spellchecker\spellchecker.php*(2.75K)(Date dernière modif. August 31 2024 15:58:02.)*02a34ca91ceeb0563ed7616722c9d17d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1992** du fichier; voici le contexte :
2. hecker.engine', 'browser', 'browser');
3. if (($engine === 'pspell' || $engine === 'pspell**shell**') && function\_exists('pspell\_new')) {
4. $classname = 'PSpell';

$conf

×

1. D:\wamp64\www\randophil.J5\components\com\_users\src\Controller\UserController.php*(8.47K)(Date dernière modif. August 27 2024 02:31:12.)*b4fc08bb1d167d56161ff16583aeed2f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1068** du fichier; voici le contexte :
2. estMethod();
3. // Populate the data array:
4. $data = [];
5. $data['return'] = **base64\_decode**($input->get('return', '', 'BASE64'));

$data['username'] = $input->get('username', '', 'USE

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4414** du fichier; voici le contexte :

idate that it is internal.

$return = $input->get('return', '', 'BASE64');

$return = **base64\_decode**($return);

// Check for a simple menu item id

if (is\_numeric($return)) {

×

1. D:\wamp64\www\randophil.J5\components\com\_users\src\Model\LoginModel.php*(4.12K)(Date dernière modif. August 27 2024 02:31:12.)*1c4f579aaad5cd4f7e8e0aacbd15e835**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2065** du fichier; voici le contexte :
2. st first
3. if ($return = $input->get('return', '', 'BASE64')) {
4. $data['return'] = **base64\_decode**($return);
5. if (!Uri::isInternal($data['return'])) {

$data['return'] = '

×

1. D:\wamp64\www\randophil.J5\components\com\_users\tmpl\method\backupcodes.php*(2.48K)(Date dernière modif. August 27 2024 02:31:12.)*d4f36a122592a71b51c93afebd1f084d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **696** du fichier; voici le contexte :
2. splay&user\_id=' . $this->user->id);
3. if (!empty($this->returnURL)) {
4. $cancelURL = $this->escape(**base64\_decode**($this->returnURL));
5. }
6. if ($this->record->method != 'backupcodes') {

throw new RuntimeException

×

1. D:\wamp64\www\randophil.J5\components\com\_users\tmpl\method\edit.php*(7.67K)(Date dernière modif. August 27 2024 02:31:12.)*137289c5894cd65afb807130c5a0be5f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **655** du fichier; voici le contexte :
2. splay&user\_id=' . $this->user->id);
3. if (!empty($this->returnURL)) {
4. $cancelURL = $this->escape(**base64\_decode**($this->returnURL));
5. }
6. $recordId = (int) $this->record->id ?? 0;

$method = $this->record-

×

1. D:\wamp64\www\randophil.J5\libraries\allediaframework\Framework\Color.php*(11.68K)(Date dernière modif. July 02 2024 08:52:14.)*1122d7cc7ccad5915d61f8c6a368ea89**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6595** du fichier; voici le contexte :
2. 'sandybrown' => '#F4A460',
3. 'seagreen' => '#2E8B57',
4. 'sea**shell**' => '#FFF5EE',
5. 'sienna' => '#A0522D',

'silver'

×

1. D:\wamp64\www\randophil.J5\libraries\allediaframework\Framework\Joomla\Controller\TraitController.php*(3.63K)(Date dernière modif. July 02 2024 08:52:14.)*4e0fcf1ca91e877134c13551a08ec1be**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2012** du fichier; voici le contexte :
2. $url = $return ?: $this->app->input->getBase64('return');
3. if ($url) {
4. $url = **base64\_decode**($url);
5. } else {
6. $url = new Uri('index.php');

if ($itemId = $this-

×

1. D:\wamp64\www\randophil.J5\libraries\src\Application\CLI\Output\Processor\ColorProcessor.php*(4.53K)(Date dernière modif. August 27 2024 02:31:12.)*d5977cfc2fb77336a54b1089e8c20355**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1579** du fichier; voici le contexte :
2. if ($noColors === null) {
3. /\*
4. \* By default windows cmd.exe and Power**Shell** does not support ANSI-colored output

\* if the variable is not set explicitly colors sh

×

1. D:\wamp64\www\randophil.J5\libraries\src\Encrypt\Aes.php*(8.62K)(Date dernière modif. August 27 2024 02:31:12.)*bce8aa9e3f20a3c09aa2d3f9ed4149f8**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5016** du fichier; voici le contexte :
2. oDecrypt, $base64encoded = true)
3. {
4. if ($base64encoded) {
5. $stringToDecrypt = **base64\_decode**($stringToDecrypt);
6. }
7. // Extract IV

$iv\_size = $this->adapter->getBlockSize

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5866** du fichier; voici le contexte :

tion\_exists('base64\_encode')) {

return false;

}

if (!\function\_exists('**base64\_decode**')) {

return false;

}

if (!\function\_exists('hash\_algos')) {

×

1. D:\wamp64\www\randophil.J5\libraries\src\Environment\Browser.php*(25.70K)(Date dernière modif. August 27 2024 02:31:12.)*52d9f026828d56555824f832f5ca1a60**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **ia\_archiver**Trouvé en position **2562** du fichier; voici le contexte :
2. 'convera',
3. 'seekbot',
4. 'Gigabot',
5. 'Gigablast',
6. 'exabot',
7. '**ia\_archiver**',
8. 'GingerCrawler',
9. 'webmon ',
10. 'HTTrack',
11. 'grub.org',

'Usine

×

1. D:\wamp64\www\randophil.J5\libraries\src\Filesystem\Stream.php*(41.73K)(Date dernière modif. August 27 2024 02:31:12.)*83df4715c8c428ec57766c2ed391781d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzget**Trouvé en position **14002** du fichier; voici le contexte :
2. switch ($this->processingmethod) {
3. case 'gz':
4. $res = $length ? **gzget**s($this->fh, $length) : **gzget**s($this->fh);
5. break;

case 'bz':

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzget**Trouvé en position **14031** du fichier; voici le contexte :

ssingmethod) {

case 'gz':

$res = $length ? **gzget**s($this->fh, $length) : **gzget**s($this->fh);

break;

case 'bz':

case 'f':

defau

×

1. D:\wamp64\www\randophil.J5\libraries\src\Helper\CMSHelper.php*(3.72K)(Date dernière modif. August 27 2024 02:31:12.)*88f8b5530ef5cdfa6dce9562d124534a**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **1365** du fichier; voici le contexte :
2. $pluginParams = new Registry($plugin->params);
3. if ((int) $pluginParams->get('lang**\_cookie**', 1) === 1) {

$langCode = $app->getInput()->cookie->getString(ApplicationHelper::ge

×

1. D:\wamp64\www\randophil.J5\libraries\src\Helper\ContentHelper.php*(8.46K)(Date dernière modif. August 27 2024 02:31:12.)*89fcaeb7d7718473a1b824e3e34d0c28**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **6970** du fichier; voici le contexte :
2. $pluginParams = new Registry($plugin->params);
3. if ((int) $pluginParams->get('lang**\_cookie**', 1) === 1) {

$langCode = $app->getInput()->cookie->getString(ApplicationHelper::ge

×

1. D:\wamp64\www\randophil.J5\libraries\src\Input\Cookie.php*(5.14K)(Date dernière modif. August 27 2024 02:31:12.)*cf286ff9945b1769efd86e21a3078f42**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1181** du fichier; voici le contexte :
2. er = InputFilter::getInstance();
3. }
4. // Set the data source.
5. $this->data = &$**\_COOKIE**;
6. // Set the options for the class.
7. $this->options = $options;
8. }

/\*\*

×

1. D:\wamp64\www\randophil.J5\libraries\src\MVC\Controller\FormController.php*(28.90K)(Date dernière modif. August 27 2024 02:31:12.)*856970c4e0222fb496105226db31b6a7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10569** du fichier; voici le contexte :
2. n = $this->input->get('return', null, 'base64');
3. if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {
4. $url = **base64\_decode**($return);
5. }

// Redirect to the list

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **10615** du fichier; voici le contexte :

);

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this->setRedirect(Route::\_($u

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **25757** du fichier; voici le contexte :

s->input->get('return', null, 'base64');

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **25811** du fichier; voici le contexte :

if (!\is\_null($return) && Uri::isInternal(**base64\_decode**($return))) {

$url = **base64\_decode**($return);

}

// Redirect to the list screen.

$this-

×

1. D:\wamp64\www\randophil.J5\libraries\src\Session\Storage\JoomlaStorage.php*(7.35K)(Date dernière modif. August 27 2024 02:31:12.)*de6a632e35893a73454ec69246ed18aa**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **1748** du fichier; voici le contexte :
2. // Disable transparent sid support and default use cookies
3. $options += [
4. 'use**\_cookie**s' => 1,
5. 'use\_trans\_sid' => 0,
6. ];

if (!headers\_sent() && !$this->isAc

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **2946** du fichier; voici le contexte :

fault behavior),

\* then the session cookie must be deleted.

\*/

if (isset($**\_COOKIE**[$session\_name])) {

$cookie = session\_get\_cookie\_params();

setcookie($sessio

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **3006** du fichier; voici le contexte :

deleted.

\*/

if (isset($\_COOKIE[$session\_name])) {

$cookie = session\_get**\_cookie**\_params();

setcookie($session\_name, '', time() - 42000, $this->cookiePath, $this->cookie

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **5638** du fichier; voici le contexte :

(headers\_sent() || $this->isActive()) {

return;

}

$cookie = session\_get**\_cookie**\_params();

if ($this->forceSSL) {

$cookie['secure'] = true;

}

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **5962** du fichier; voici le contexte :

cookiePath !== '') {

$cookie['path'] = $this->cookiePath;

}

session\_set**\_cookie**\_params($cookie['lifetime'], $cookie['path'], $cookie['domain'], $cookie['secure'], true);

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **7472** du fichier; voici le contexte :

a from the session

if (!empty($\_SESSION['joomla'])) {

$this->data = unserialize(**base64\_decode**($\_SESSION['joomla']));

}

}

}

×

1. D:\wamp64\www\randophil.J5\libraries\src\User\User.php*(25.26K)(Date dernière modif. August 27 2024 02:31:12.)*749010835d98ea00e4fb023badf538ed**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **Brute force**Trouvé en position **10154** du fichier; voici le contexte :
2. e 1.7.0
3. \*/
4. public function getAuthorisedCategories($component, $action)
5. {
6. // **Brute force** method: get all published category rows for the component and check each one

// @todo: Modi

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\algo26-matthias\idna-convert\LICENSE*(25.84K)(Date dernière modif. March 18 2024 18:24:08.)*40d2542b8c43a3ec2b7f5da31a697b88**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Hacker**Trouvé en position **26356** du fichier; voici le contexte :
2. copyright interest in the
3. library `Frob' (a library for tweaking knobs) written by James Random
4. **Hacker**.
5. {signature of Ty Coon}, 1 April 1990
6. Ty Coon, President of Vice

That's all there is to it!

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\algo26-matthias\idna-convert\src\TranscodeUnicode\TranscodeUnicode.php*(13.74K)(Date dernière modif. March 18 2024 18:24:08.)*94f821d48e0b7414d579ef39bcc0d3ac**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9603** du fichier; voici le contexte :
2. continue;
3. }
4. }
5. $tmp = **base64\_decode**($b64);
6. $tmp = substr($tmp, -1 \* (strlen($tmp) % 2));

for ($

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\composer\autoload\_files.php*(5.27K)(Date dernière modif. August 27 2024 02:32:50.)*c1a203568b8b24fa81dc2b712d4b2b9b**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **2801** du fichier; voici le contexte :
2. 'd02cf21124526632320d6f20b1bbf905' => $vendorDir . '/laminas/laminas-diactoros/src/functions/parse**\_cookie**\_header.php',

'd919fc9d5ad52cfb7f322f7fe36458ab' => $vendorDir . '/laminas/laminas-diactoros/src

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **3865** du fichier; voici le contexte :

'751a5a3f463e4be759be31748b61737c' => $vendorDir . '/laminas/laminas-diactoros/src/functions/parse**\_cookie**\_header.legacy.php',

'320cde22f66dd4f5d3fd621d3e88b98f' => $vendorDir . '/symfony/polyfill-ctype

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\composer\autoload\_static.php*(480.06K)(Date dernière modif. August 27 2024 02:32:50.)*d4d1636afecab7c4359bbedfdf02f3f5**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **3064** du fichier; voici le contexte :
2. 2cf21124526632320d6f20b1bbf905' => \_\_DIR\_\_ . '/..' . '/laminas/laminas-diactoros/src/functions/parse**\_cookie**\_header.php',

'd919fc9d5ad52cfb7f322f7fe36458ab' => \_\_DIR\_\_ . '/..' . '/laminas/laminas-diac

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **4200** du fichier; voici le contexte :

1a5a3f463e4be759be31748b61737c' => \_\_DIR\_\_ . '/..' . '/laminas/laminas-diactoros/src/functions/parse**\_cookie**\_header.legacy.php',

'320cde22f66dd4f5d3fd621d3e88b98f' => \_\_DIR\_\_ . '/..' . '/symfony/polyf

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\composer\ca-bundle\res\cacert.pem*(224.27K)(Date dernière modif. March 15 2024 16:00:32.)*594084120d27f482b1dc48f558d12d48**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **45420** du fichier; voici le contexte :
2. CzAJBgNVBAYTAlVTMRAw
3. DgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxTdGFyZmllbGQg
4. VG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMuMTIwMAYDVQQDEylTdGFyZmllbGQgUm9vdCBDZXJ0aWZpY2F0ZSBB

dXRob3JpdHkgLSBHMjCCASIwDQYJK

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **46931** du fichier; voici le contexte :

CzAJBgNV

BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxT

dGFyZmllbGQgVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMuMTswOQYDVQQDEzJTdGFyZmllbGQgU2VydmljZXMg

Um9vdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgLSBHM

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **N5c3Rlb**Trouvé en position **56243** du fichier; voici le contexte :

0Q0EyMB4XDTA5MDUyOTA1MDAzOVoXDTI5MDUyOTA1MDAzOVowXTELMAkGA1UEBhMC

SlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">N5c3Rlb**XMgQ08uLExURC4xJzAlBgNVBAsTHlNlY3Vy

aXR5IENvbW11bmljYXRpb24gUm9vdENBMjCCASIwDQYJKoZIhvcNAQEBBQADggEP

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **109420** du fichier; voici le contexte :

gAwIBAgIQIdbQSk8lD8kyN/yqXhKN6TANBgkqhkiG9w0BAQ0FADCBgDELMAkGA1UE

BhMCUEwxIjAgBgNVBAoTGVVuaXpldG8gVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzIFMuQS4xJzAlBgNVBAsTHkNlcnR1

bSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTEkMCIGA1UEAxMbQ2VydHVtIFRyd

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **N5c3Rlb**Trouvé en position **205764** du fichier; voici le contexte :

0Q0ExMB4XDTE2MDYxNjA1MTUyOFoXDTM4MDExODA1MTUyOFowYTEL

MAkGA1UEBhMCSlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">N5c3Rlb**XMgQ08uLExURC4xKzApBgNV

BAMTIlNlY3VyaXR5IENvbW11bmljYXRpb24gRUNDIFJvb3RDQTEwdjAQBgcqhkjOPQIBBgUrgQQA

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **218276** du fichier; voici le contexte :

DQSBHMzAeFw0yMTA1MjAwMjEwMTlaFw00NjA1MTkwMjEw

MTlaMFoxCzAJBgNVBAYTAkNOMSUwIwYDVQQKDBxUcnVzdEFzaWEgVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMu

MSQwIgYDVQQDDBtUcnVzdEFzaWEgR2xvYmFsIFJvb3QgQ0EgRzMwggIiMA0GCSqGSIb3DQEBAQUA

A4IC

**Attention** Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral; certains mots clefs PHP comme "eval" ou "system" p.ex. permettent l'exécution d'un code et la signature qui est mentionnée ici peut-être risquée. Pour décoder du code base64, vous pouvez utiliser différents décodeur "base64\_decode" disponible sur le net dont p.ex. https://base64.avonture.be/Signature : **VjaG**Trouvé en position **220341** du fichier; voici le contexte :

DQSBHNDAeFw0yMTA1MjAwMjEwMjJaFw00NjA1MTkwMjEwMjJa

MFoxCzAJBgNVBAYTAkNOMSUwIwYDVQQKDBxUcnVzdEFzaWEgVG**<="" span="" data-original-title="" title="" style="box-sizing: border-box; font-weight: 700; text-decoration: underline; border-bottom: 1px solid rgb(0, 0, 0); color: red;">">VjaG**5vbG9naWVzLCBJbmMuMSQw

IgYDVQQDDBtUcnVzdEFzaWEgR2xvYmFsIFJvb3QgQ0EgRzQwdjAQBgcqhkjOPQIBBgUrgQQAIgNi

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\defuse\php-encryption\dist\Makefile*(1.04K)(Date dernière modif. June 19 2023 10:10:36.)*8a6965d45479ea87e48f57ce2cbb1dd2**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **166** du fichier; voici le contexte :
2. `composer`
3. # must be installed and in your $PATH. Run it from inside the dist/ directory.
4. box := $(**shell** which box)
5. composer := $(**shell** which composer)
6. gitcommit := $(**shell** git rev-parse HEAD)

.PHONY: al

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **197** du fichier; voici le contexte :

and in your $PATH. Run it from inside the dist/ directory.

box := $(**shell** which box)

composer := $(**shell** which composer)

gitcommit := $(**shell** git rev-parse HEAD)

.PHONY: all

all: build-phar

.PHONY: sign

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **234** du fichier; voici le contexte :

the dist/ directory.

box := $(**shell** which box)

composer := $(**shell** which composer)

gitcommit := $(**shell** git rev-parse HEAD)

.PHONY: all

all: build-phar

.PHONY: sign-phar

sign-phar:

gpg -u DD2E507F7BDB

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **549** du fichier; voici le contexte :

xport git tree and run there.

.PHONY: build-phar

build-phar:

@echo "Creating .phar from revision $(**shell** git rev-parse HEAD)."

rm -rf worktree

install -d worktree

(cd $(CURDIR)/..; git archive HEAD) |

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\defuse\php-encryption\src\Crypto.php*(14.26K)(Date dernière modif. June 19 2023 10:10:36.)*50bd1417f92279bf4041de425e0151b2**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **1284** du fichier; voici le contexte :
2. \* Encrypts a string with a password, using a slow key derivation function
3. \* to make password **cracking** more expensive.
4. \*
5. \* @param string $plaintext
6. \* @param string $password

\* @param

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **3747** du fichier; voici le contexte :

iphertext to a string with a password, using a slow key

\* derivation function to make password **cracking** more expensive.

\*

\* @param string $ciphertext

\* @param string $password

\* @para

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\defuse\php-encryption\src\File.php*(26.91K)(Date dernière modif. June 19 2023 10:10:36.)*c81dc5b5096c317b714ecb8a09082fca**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **742** du fichier; voici le contexte :
2. \* Encrypts a file with a password, using a slow key derivation function to
3. \* make password **cracking** more expensive.
4. \*
5. \* @param string $inputFilename

\* @param string $outputFilename

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **2028** du fichier; voici le contexte :

\* Decrypts a file with a password, using a slow key derivation function to

\* make password **cracking** more expensive.

\*

\* @param string $inputFilename

\* @param string $outputFilename

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **3432** du fichier; voici le contexte :

e handle into another with a

\* password, using a slow key derivation function to make password **cracking**

\* more expensive.

\*

\* @param resource $inputHandle

\* @param resource $outputHan

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **4867** du fichier; voici le contexte :

resource into another with a password, using

\* a slow key derivation function to make password **cracking** more expensive.

\*

\* @param resource $inputHandle

\* @param resource $outputHandle

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\guzzlehttp\promises\LICENSE*(1.25K)(Date dernière modif. May 21 2023 16:31:44.)*8035eaaec6b3b562c1aed15adc8b908a**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature :**<hell< strong="" style="box-sizing: border-box;"></hell<>Trouvé en position 115 du fichier; voici le contexte :**
2. (MIT)
3. Copyright (c) 2015 Michael Dowling <mtdowling@gmail.com>
4. Copyright (c) 2015 Graham Campbell <hello@gjcampbell.co.uk>
5. Copyright (c) 2017 Tobias Schultze <webmaster@tubo-world.de>

Copyright (c) 2020

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\guzzlehttp\psr7\LICENSE*(1.37K)(Date dernière modif. December 03 2023 22:05:36.)*db7096d1ec87ffcdc25c249bcf336120**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature :**<hell< strong="" style="box-sizing: border-box;"></hell<>Trouvé en position 180 du fichier; voici le contexte :**
2. Copyright (c) 2015 Márk Sági-Kazár <mark.sagikazar@gmail.com>
3. Copyright (c) 2015 Graham Campbell <hello@gjcampbell.co.uk>
4. Copyright (c) 2016 Tobias Schultze <webmaster@tubo-world.de>

Copyright (c) 2016

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\guzzlehttp\psr7\src\ServerRequest.php*(9.33K)(Date dernière modif. December 03 2023 22:05:36.)*95f6e1f9e5e86234995e36032d3ee249**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **4817** du fichier; voici le contexte :
2. /\*\*
3. \* Return a ServerRequest populated with superglobals:
4. \* $\_GET
5. \* $\_POST
6. \* $**\_COOKIE**
7. \* $\_FILES
8. \* $\_SERVER
9. \*/

public static function fromGlobals(): ServerRequestInter

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5425** du fichier; voici le contexte :

eaders, $body, $protocol, $\_SERVER);

return $serverRequest

->withCookieParams($**\_COOKIE**)

->withQueryParams($\_GET)

->withParsedBody($\_POST)

->withUpload

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\jfcherng\php-diff\src\Renderer\Html\Combined.php*(15.70K)(Date dernière modif. March 10 2024 19:40:30.)*27126f14eb742c57901c7ae18a243ca0**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **"Hell**Trouvé en position **10097** du fichier; voici le contexte :
2. h as
3. \* extract information for "<ins>part 1</ins>" and "<ins>part 2</ins>"
4. \* from **"Hell**o <ins>part 1</ins>SOME OTHER TEXT<ins>part 2</ins> World"
5. \*

\* @param string $line t

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\joomla\archive\src\Zip.php*(19.53K)(Date dernière modif. August 15 2024 21:52:52.)*d3b0809f28021da3d328e20a45d659b2**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzcompress**Trouvé en position **16405** du fichier; voici le contexte :
2. eader" segment.
3. $uncLen = \strlen($data);
4. $crc = crc32($data);
5. $zdata = **gzcompress**($data);
6. $zdata = substr(substr($zdata, 0, -4), 2);

$cLen = \strlen($zdata);

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\joomla\database\src\Pgsql\PgsqlDriver.php*(32.79K)(Date dernière modif. August 15 2024 14:09:54.)*d875d9d54aa294fd5764ea52d168f49a**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **SQL injection**Trouvé en position **9454** du fichier; voici le contexte :
2. tTableKeys($table)
3. {
4. $this->connect();
5. // To check if table exists and prevent **SQL injection**
6. $tableList = $this->getTableList();

$tableSub = $this->replacePrefix($table);

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **SQL injection**Trouvé en position **12539** du fichier; voici le contexte :

public function getTableSequences($table)

{

// To check if table exists and prevent **SQL injection**

$tableList = $this->getTableList();

$tableSub = $this->replacePrefix($table);

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **SQL injection**Trouvé en position **16312** du fichier; voici le contexte :

$newTable = $this->replacePrefix($newTable);

// To check if table exists and prevent **SQL injection**

$tableList = $this->getTableList();

// Origin Table does not exist

if (!\i

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\joomla\filesystem\src\Stream.php*(38.57K)(Date dernière modif. August 16 2024 13:41:56.)*bf79fa6c3b9056d791890f21ea318a7c**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzget**Trouvé en position **12476** du fichier; voici le contexte :
2. switch ($this->processingmethod) {
3. case 'gz':
4. $res = $length ? **gzget**s($this->fh, $length) : **gzget**s($this->fh);
5. break;

case 'bz':

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzget**Trouvé en position **12505** du fichier; voici le contexte :

ssingmethod) {

case 'gz':

$res = $length ? **gzget**s($this->fh, $length) : **gzget**s($this->fh);

break;

case 'bz':

case 'f':

defa

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\joomla\input\src\Cookie.php*(3.90K)(Date dernière modif. October 08 2023 01:27:36.)*4e3823d75dbb81101b334af26341c360**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **445** du fichier; voici le contexte :
2. \* Constructor.
3. \*
4. \* @param array|null $source Source data (Optional, default is $**\_COOKIE**)
5. \* @param array $options Array of configuration parameters (Optional)
6. \*

\* @

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **677** du fichier; voici le contexte :

ublic function \_\_construct($source = null, array $options = [])

{

$source = $source ?? $**\_COOKIE**;

parent::\_\_construct($source, $options);

}

/\*\*

\* Sets a value

\*

\* @

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\joomla\session\src\Storage\NativeStorage.php*(10.65K)(Date dernière modif. August 16 2024 13:17:14.)*55a01eb7f69c19d72ca0fffce4af7953**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **1479** du fichier; voici le contexte :
2. // Disable transparent sid support and default use cookies
3. $options += [
4. 'use**\_cookie**s' => 1,
5. 'use\_trans\_sid' => 0,
6. ];

if (!headers\_sent()) {

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **9502** du fichier; voici le contexte :

gc\_probability', 'lazy\_write', 'name', 'referer\_check', 'serialize\_handler', 'use\_strict\_mode', 'use**\_cookie**s',

'use\_only**\_cookie**s', 'use\_trans\_sid', 'upload\_progress.enabled', 'upload\_progress

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **9538** du fichier; voici le contexte :

', 'referer\_check', 'serialize\_handler', 'use\_strict\_mode', 'use**\_cookie**s',

'use\_only**\_cookie**s', 'use\_trans\_sid', 'upload\_progress.enabled', 'upload\_progress.cleanup', 'upload\_progress.prefix',

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **10451** du fichier; voici le contexte :

'Failed to start the session: already started by PHP.');

}

if (ini\_get('session.use**\_cookie**s') && headers\_sent($file, $line)) {

throw new \RuntimeException(

sprint

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\laminas\laminas-diactoros\src\ServerRequestFactory.php*(3.15K)(Date dernière modif. October 29 2023 18:17:44.)*7195f0d58af897f1032d7e5e6ac8072b**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1238** du fichier; voici le contexte :
2. $query $\_GET superglobal
3. \* @param array $body $\_POST superglobal
4. \* @param array $cookies $**\_COOKIE** superglobal
5. \* @param array $files $\_FILES superglobal

\* @param null|FilterServerRequestIn

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **2726** du fichier; voici le contexte :

lMethodFromSapi($server),

'php://input',

$headers,

$cookies ?: $**\_COOKIE**,

$query ?: $\_GET,

$body ?: $\_POST,

marshalProtocolVersionFromSa

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\lcobucci\jwt\src\SodiumBase64Polyfill.php*(2.54K)(Date dernière modif. January 02 2023 15:28:00.)*4c69d0db30c4f65d8ef7a553ebed6ad0**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **139** du fichier; voici le contexte :
2. ce Lcobucci\JWT;
3. use Lcobucci\JWT\Encoding\CannotDecodeContent;
4. use SodiumException;
5. use function **base64\_decode**;
6. use function base64\_encode;
7. use function function\_exists;
8. use function is\_string;

use function rtr

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2424** du fichier; voici le contexte :

DDING

) {

$encoded = strtr($encoded, '-\_', '+/');

}

$decoded = **base64\_decode**($encoded, true);

if (! is\_string($decoded)) {

throw CannotDecodeContent::inval

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\maximebf\debugbar\src\DebugBar\DataCollector\AggregatedCollector.php*(4.11K)(Date dernière modif. March 12 2024 16:23:08.)*1dd1c50a4539acdd9a15c2addc635d25**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'hell**Trouvé en position **592** du fichier; voici le contexte :
2. \* $aggcollector->addCollector(new MessagesCollector('msg2'));
3. \* $aggcollector['msg1']->addMessage(**'hell**o world');
4. \* </code>
5. \*/
6. class AggregatedCollector implements DataCollectorInterface, ArrayAccess

{

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\maximebf\debugbar\src\DebugBar\DataCollector\RequestDataCollector.php*(1.70K)(Date dernière modif. March 12 2024 16:23:08.)*2ac9499be4ac7d0d0df99c6df084fb0f**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **529** du fichier; voici le contexte :
2. ray
3. \*/
4. public function collect()
5. {
6. $vars = array('\_GET', '\_POST', '\_SESSION', '**\_COOKIE**');
7. $data = array();
8. foreach ($vars as $var) {

if (isset($GLOBALS[$var]

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\paragonie\sodium\_compat\src\Compat.php*(146.69K)(Date dernière modif. April 30 2023 04:54:54.)*1a1116a0b0df0f22bd91d0980d4336ba**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Hell**Trouvé en position **40223** du fichier; voici le contexte :
2. essages.
3. \*
4. \* Algorithm: X25519-XSalsa20-Poly1305.
5. \* X25519: Elliptic-Curve Diffie **Hell**man over Curve25519.
6. \* XSalsa20: Extended-nonce variant of salsa20.

\* Poyl1305: Po

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\php-tuf\php-tuf\tests\Unit\CanonicalJsonTraitTest.php*(3.16K)(Date dernière modif. March 11 2024 21:10:08.)*8356e93d121e88c74eddd384455c5f0d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'Hell**Trouvé en position **1010** du fichier; voici le contexte :
2. // alphabetically (which is what we're trying to avoid).
3. 'b' => array\_fill(0, 20, **'Hell**o!'),
4. 'a' => 'Canonically speaking, I go before b.',

// This should be sorte

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\php-tuf\php-tuf\tests\Unit\FileStorageTest.php*(5.03K)(Date dernière modif. March 11 2024 21:10:08.)*9d299753722ab3a3636f17a0431d6b21**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **3476** du fichier; voici le contexte :
2. );
3. $metadata->getRole()->willReturn($role);
4. $metadata->getSource()->willReturn("From **hell**'s heart, I refactor thee!");
5. $metadata->ensureIsTrusted()->shouldBeCalled();

$stora

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **3740** du fichier; voici le contexte :

'/' . $expectedFileName;

$this->assertFileExists($filePath);

$this->assertSame("From **hell**'s heart, I refactor thee!", file\_get\_contents($filePath));

$storage->delete($role);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'hell**Trouvé en position **4417** du fichier; voici le contexte :

>getRoot();

}

public function testFileNamesAreUrlEncoded(): void

{

$roleName = **'hell**o/../there!';

$fileContents = '{["A test of your mettle"]}';

$dir = sys\_get\_temp\_di

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'hell**Trouvé en position **4872** du fichier; voici le contexte :

sted()->shouldBeCalled();

$storage->save($metadata->reveal());

$expectedFileName = **'hell**o%2F..%2Fthere%21.json';

$this->assertFileExists($dir . '/' . $expectedFileName);

$

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpmailer\phpmailer\LICENSE*(25.91K)(Date dernière modif. November 26 2023 00:23:28.)*23c2a5e0106b99d75238986559bb5fc6**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Hacker**Trouvé en position **26425** du fichier; voici le contexte :
2. l copyright interest in the
3. library `Frob' (a library for tweaking knobs) written by James Random **Hacker**.
4. <signature of Ty Coon>, 1 April 1990
5. Ty Coon, President of Vice

That's all there is to it!

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpmailer\phpmailer\src\PHPMailer.php*(178.88K)(Date dernière modif. November 26 2023 00:23:28.)*f0632be418408bccb5bbe6734bb5ec8f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **152356** du fichier; voici le contexte :
2. if (count($match) === 4 && static::ENCODING\_BASE64 === $match[2]) {
3. $data = **base64\_decode**($match[3]);
4. } elseif ('' === $match[2]) {

$data = rawur

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **55919** du fichier; voici le contexte :

be escaped.

if (!empty($this->Sender) && static::validateAddress($this->Sender) && self::is**Shell**Safe($this->Sender)) {

if ($this->Mailer === 'qmail') {

$sendmailFmt = '

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **56562** du fichier; voici le contexte :

$sendmailFmt = '%s -oi -t';

}

$sendmail = sprintf($sendmailFmt, escape**shell**cmd($this->Sendmail), $this->Sender);

$this->edebug('Sendmail path: ' . $this->Sendmail);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **58933** du fichier; voici le contexte :

true;

}

/\*\*

\* Fix CVE-2016-10033 and CVE-2016-10045 by disallowing potentially unsafe **shell** characters.

\* Note that escape**shell**arg and escape**shell**cmd are inadequate for our purposes, esp

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **58974** du fichier; voici le contexte :

10033 and CVE-2016-10045 by disallowing potentially unsafe **shell** characters.

\* Note that escape**shell**arg and escape**shell**cmd are inadequate for our purposes, especially on Windows.

\*

\* @see ht

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **58993** du fichier; voici le contexte :

10045 by disallowing potentially unsafe **shell** characters.

\* Note that escape**shell**arg and escape**shell**cmd are inadequate for our purposes, especially on Windows.

\*

\* @see https://github.com/PH

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **59283** du fichier; voici le contexte :

tring The string to be validated

\*

\* @return bool

\*/

protected static function is**Shell**Safe($string)

{

//It's not possible to use shell commands safely (which includes the mai

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **59343** du fichier; voici le contexte :

\*/

protected static function isShellSafe($string)

{

//It's not possible to use **shell** commands safely (which includes the mail() function) without escape**shell**arg,

//but some hos

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **59416** du fichier; voici le contexte :

//It's not possible to use **shell** commands safely (which includes the mail() function) without escape**shell**arg,

//but some hosting providers disable it, creating a security problem that we don't want

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **59603** du fichier; voici le contexte :

that we don't want to have to deal with,

//so we don't.

if (!function\_exists('escape**shell**arg') || !function\_exists('escape**shell**cmd')) {

return false;

}

if (

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **59641** du fichier; voici le contexte :

h,

//so we don't.

if (!function\_exists('escape**shell**arg') || !function\_exists('escape**shell**cmd')) {

return false;

}

if (

escape**shell**cmd($string) !== $

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **59723** du fichier; voici le contexte :

ion\_exists('escape**shell**cmd')) {

return false;

}

if (

escape**shell**cmd($string) !== $string

|| !in\_array(escape**shell**arg($string), ["'$string'", "\"$string\

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **59784** du fichier; voici le contexte :

}

if (

escape**shell**cmd($string) !== $string

|| !in\_array(escape**shell**arg($string), ["'$string'", "\"$string\""])

) {

return false;

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **60073** du fichier; voici le contexte :

$c = $string[$i];

//All other characters have a special meaning in at least one common **shell**, including = and +.

//Full stop (.) has a special meaning in cmd.exe, but its impact sh

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **63474** du fichier; voici le contexte :

if (!empty($this->Sender) && static::validateAddress($this->Sender)) {

if (self::is**Shell**Safe($this->Sender)) {

$params = sprintf('-f%s', $this->Sender);

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **72935** du fichier; voici le contexte :

, $options)) {

try {

if ($this->Helo) {

**$hell**o = $this->Helo;

} else {

**$hell**o = $this->serverHostname

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **73010** du fichier; voici le contexte :

**$hell**o = $this->Helo;

} else {

**$hell**o = $this->serverHostname();

}

$this->smtp->hello(**$hell**o);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **>hell**Trouvé en position **73098** du fichier; voici le contexte :

$hello = $this->serverHostname();

}

$this->smtp-**>hell**o($hello);

//Automatically enable TLS encryption if:

//\* it'

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **73105** du fichier; voici le contexte :

**$hell**o = $this->serverHostname();

}

$this->smtp->hello(**$hell**o);

//Automatically enable TLS encryption if:

//\* it's not d

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **>hell**Trouvé en position **74142** du fichier; voici le contexte :

//We must resend EHLO after TLS negotiation

$this->smtp-**>hell**o($hello);

}

if (

$this->SMTPAuth &&

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **74149** du fichier; voici le contexte :

//We must resend EHLO after TLS negotiation

$this->smtp->hello(**$hell**o);

}

if (

$this->SMTPAuth && !$this

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpmailer\phpmailer\src\SMTP.php*(47.37K)(Date dernière modif. November 26 2023 00:23:28.)*9ca45351c23c33c9e9ae6d5d75acb3a7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **19868** du fichier; voici le contexte :
2. return false;
3. }
4. //Get the challenge
5. $challenge = **base64\_decode**(substr($this->last\_reply, 4));
6. //Build the response

$response = $u

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **15484** du fichier; voici le contexte :

eturn (bool) $crypto\_ok;

}

/\*\*

\* Perform SMTP authentication.

\* Must be run after **hell**o().

\*

\* @see  **hell**o()

\*

\* @param string $username The user name

\* @param

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **15515** du fichier; voici le contexte :

/\*\*

\* Perform SMTP authentication.

\* Must be run after **hell**o().

\*

\* @see  **hell**o()

\*

\* @param string $username The user name

\* @param string $password The password

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **27645** du fichier; voici le contexte :

tring $host The host name or IP to connect to

\*

\* @return bool

\*/

public function **hell**o($host = '')

{

//Try extended **hell**o first (RFC 2821)

if ($this->sendHello('EHLO

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **27692** du fichier; voici le contexte :

\*

\* @return bool

\*/

public function **hell**o($host = '')

{

//Try extended **hell**o first (RFC 2821)

if ($this->sendHello('EHLO', $host)) {

return true;

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **dHell**Trouvé en position **27738** du fichier; voici le contexte :

unction hello($host = '')

{

//Try extended hello first (RFC 2821)

if ($this->sen**dHell**o('EHLO', $host)) {

return true;

}

//Some servers shut down the SMTP se

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **dHell**Trouvé en position **27982** du fichier; voici le contexte :

r($this->helo\_rply, 0, 3) == '421') {

return false;

}

return $this->sen**dHell**o('HELO', $host);

}

/\*\*

\* Send an SMTP HELO or EHLO command.

\* Low-level implemen

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **28101** du fichier; voici le contexte :

t);

}

/\*\*

\* Send an SMTP HELO or EHLO command.

\* Low-level implementation used by **hell**o().

\*

\* @param string $hello The HELO string

\* @param string $host The hostname to

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **28139** du fichier; voici le contexte :

HELO or EHLO command.

\* Low-level implementation used by hello().

\*

\* @param string **$hell**o The HELO string

\* @param string $host The hostname to say we are

\*

\* @return bool

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hell**Trouvé en position **28262** du fichier; voici le contexte :

\* @param string $host The hostname to say we are

\*

\* @return bool

\*

\* @see **hell**o()

\*/

protected function sendHello($hello, $host)

{

$noerror = $this->sendComm

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **dHell**Trouvé en position **28305** du fichier; voici le contexte :

say we are

\*

\* @return bool

\*

\* @see hello()

\*/

protected function sen**dHell**o($hello, $host)

{

$noerror = $this->sendCommand($hello, $hello . ' ' . $host, 250);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **28312** du fichier; voici le contexte :

are

\*

\* @return bool

\*

\* @see hello()

\*/

protected function sendHello(**$hell**o, $host)

{

$noerror = $this->sendCommand(**$hell**o, **$hell**o . ' ' . $host, 250);

$t

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **28371** du fichier; voici le contexte :

\*/

protected function sendHello(**$hell**o, $host)

{

$noerror = $this->sendCommand(**$hell**o, **$hell**o . ' ' . $host, 250);

$this->helo\_rply = $this->last\_reply;

if ($noerror) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **28379** du fichier; voici le contexte :

protected function sendHello(**$hell**o, $host)

{

$noerror = $this->sendCommand(**$hell**o, **$hell**o . ' ' . $host, 250);

$this->helo\_rply = $this->last\_reply;

if ($noerror) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **eHell**Trouvé en position **28500** du fichier; voici le contexte :

250);

$this->helo\_rply = $this->last\_reply;

if ($noerror) {

$this->pars**eHell**oFields($hello);

} else {

$this->server\_caps = null;

}

return $

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **$hell**Trouvé en position **28513** du fichier; voici le contexte :

$this->helo\_rply = $this->last\_reply;

if ($noerror) {

$this->parseHelloFields(**$hell**o);

} else {

$this->server\_caps = null;

}

return $noerror;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **eHell**Trouvé en position **28872** du fichier; voici le contexte :

server name.

\*

\* @param string $type `HELO` or `EHLO`

\*/

protected function pars**eHell**oFields($type)

{

$this->server\_caps = [];

$lines = explode("\n", $this->helo\_rpl

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Common\Functions\Strings.php*(15.86K)(Date dernière modif. March 03 2024 04:14:58.)*f698d5b96b131c34a1179cad99321799**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14259** du fichier; voici le contexte :
2. ssues/39
3. \*
4. \* @param string $data
5. \* @return string
6. \*/
7. public static function **base64\_decode**($data)
8. {
9. return function\_exists('sodium\_base642bin') ?

sodium\_base642bin($d

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **14670** du fichier; voici le contexte :

urn string

\*/

public static function base64url\_decode($data)

{

// return self::**base64\_decode**(str\_replace(['-', '\_'], ['+', '/'], $data));

return function\_exists('sodium\_base642bin') ?

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\Common\Formats\Keys\OpenSSH.php*(7.62K)(Date dernière modif. March 03 2024 04:14:58.)*0a65bb5a529c118574f062af58c8daf0**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1766** du fichier; voici le contexte :
2. $key = preg\_replace('#(?:^-.\*?-[\r\n]\*$)|\s#ms', '', $key);
3. $key = Strings::**base64\_decode**($key);
4. $magic = Strings::shift($key, 15);

if ($magic != "openssh-key-v1\0")

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4188** du fichier; voici le contexte :

}

$parts = explode(' ', $key, 3);

if (!isset($parts[1])) {

$key = **base64\_decode**($parts[0]);

$comment = false;

} else {

$asciiType = $parts[0];

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4356** du fichier; voici le contexte :

se {

$asciiType = $parts[0];

self::checkType($parts[0]);

$key = **base64\_decode**($parts[1]);

$comment = isset($parts[2]) ? $parts[2] : false;

}

if ($key

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\Common\Formats\Keys\PuTTY.php*(13.07K)(Date dernière modif. March 03 2024 04:14:58.)*d33a575b78269a7b8ef4049c1fe419b4**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6587** du fichier; voici le contexte :
2. blicLength = trim(preg\_replace('#Public-Lines: (\d+)#', '$1', $key[3]));
3. $public = Strings::**base64\_decode**(implode('', array\_map('trim', array\_slice($key, 4, $publicLength))));

$source = Strings::p

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **8818** du fichier; voici le contexte :

= trim(preg\_replace('#Private-Lines: (\d+)#', '$1', $key[$offset++]));

$private = Strings::**base64\_decode**(implode('', array\_map('trim', array\_slice($key, $offset, $privateLength))));

if ($encrypti

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\Common\SymmetricKey.php*(126.00K)(Date dernière modif. March 03 2024 04:14:58.)*c31f9a763b3510dec9b9385df7f1b6dd**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **brute force**Trouvé en position **69280** du fichier; voici le contexte :
2. ll be doing CTR and less than 4 provides minimal security that could be trivially
3. // easily **brute force**d.

// see https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf#page

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\DH.php*(18.72K)(Date dernière modif. March 03 2024 04:14:58.)*d3963f0dfa9b13cdbee1acc6858b0285**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **1718** du fichier; voici le contexte :
2. resenting the size of the prime in bits (the base is assumed to be 2)
3. \* - a string (eg. diffie**-hell**man-group14-sha1)
4. \*
5. \* @return Parameters
6. \*/

public static function createParamete

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **3126** du fichier; voici le contexte :

ction-6.2 and

// http://tools.ietf.org/html/rfc2412, appendex E

case 'diffie**-hell**man-group1-sha1':

$prime = 'FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E08

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **3635** du fichier; voici le contexte :

break;

// see http://tools.ietf.org/html/rfc3526#section-3

case 'diffie**-hell**man-group14-sha1': // 2048-bit MODP Group

case 'diffie**-hell**man-group14-sha256':

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **3706** du fichier; voici le contexte :

on-3

case 'diffie**-hell**man-group14-sha1': // 2048-bit MODP Group

case 'diffie**-hell**man-group14-sha256':

$prime = 'FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **4595** du fichier; voici le contexte :

break;

// see https://tools.ietf.org/html/rfc3526#section-4

case 'diffie**-hell**man-group15-sha512': // 3072-bit MODP Group

$prime = 'FFFFFFFFFFFFFFFFC90FDAA22168C2

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **5883** du fichier; voici le contexte :

break;

// see https://tools.ietf.org/html/rfc3526#section-5

case 'diffie**-hell**man-group16-sha512': // 4096-bit MODP Group

$prime = 'FFFFFFFFFFFFFFFFC90FDAA22168C2

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **7547** du fichier; voici le contexte :

break;

// see https://tools.ietf.org/html/rfc3526#section-6

case 'diffie**-hell**man-group17-sha512': // 6144-bit MODP Group

$prime = 'FFFFFFFFFFFFFFFFC90FDAA22168C2

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **9963** du fichier; voici le contexte :

break;

// see https://tools.ietf.org/html/rfc3526#section-7

case 'diffie**-hell**man-group18-sha512': // 8192-bit MODP Group

$prime = 'FFFFFFFFFFFFFFFFC90FDAA22168C2

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\DSA\Formats\Keys\XML.php*(5.08K)(Date dernière modif. March 03 2024 04:14:58.)*886a417d24ececc0ca4696ebcbf692b7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2296** du fichier; voici le contexte :
2. emp->length) {
3. continue;
4. }
5. $value = new BigInteger(Strings::**base64\_decode**($temp->item(0)->nodeValue), 256);
6. switch ($key) {

case 'p': // a prime

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\EC\Formats\Keys\PuTTY.php*(4.39K)(Date dernière modif. March 03 2024 04:14:58.)*b7436aefdb4151fac3ad7187f168c061**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3079** du fichier; voici le contexte :
2. OpenSSH::savePublicKey($curve, $publicKey));
3. $name = $public[0];
4. $public = Strings::**base64\_decode**($public[1]);
5. list(, $length) = unpack('N', Strings::shift($public, 4));

Strings::sh

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4295** du fichier; voici le contexte :

OpenSSH::savePublicKey($curve, $publicKey));

$type = $public[0];

$public = Strings::**base64\_decode**($public[1]);

list(, $length) = unpack('N', Strings::shift($public, 4));

Strings::sh

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\EC\Formats\Keys\XML.php*(17.47K)(Date dernière modif. March 03 2024 04:14:58.)*10df3dcaef3a96b4b12be65afc528404**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4761** du fichier; voici le contexte :
2. string $value
3. \*/
4. private static function decodeValue($value)
5. {
6. return Strings::**base64\_decode**(str\_replace(["\r", "\n", ' ', "\t"], '', $value));
7. }
8. /\*\*

\* Extract points from an XML

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\Random.php*(9.30K)(Date dernière modif. March 03 2024 04:14:58.)*af21a780fc59992b916b419d9e40b2db**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **3662** du fichier; voici le contexte :
2. // save old session data
3. $old\_session\_id = session\_id();
4. $old\_use**\_cookie**s = ini\_get('session.use**\_cookie**s');

$old\_session\_cache\_limiter = session\_cache\_limiter()

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **3693** du fichier; voici le contexte :

data

$old\_session\_id = session\_id();

$old\_use**\_cookie**s = ini\_get('session.use**\_cookie**s');

$old\_session\_cache\_limiter = session\_cache\_limiter();

$\_OLD\_SESSION = i

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **3991** du fichier; voici le contexte :

session\_write\_close();

}

session\_id(1);

ini\_set('session.use**\_cookie**s', 0);

session\_cache\_limiter('');

session\_start();

$v = (isset

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **4315** du fichier; voici le contexte :

'') .

(isset($\_GET) ? self::safe\_serialize($\_GET) : '') .

(isset($**\_COOKIE**) ? self::safe\_serialize($**\_COOKIE**) : '') .

// as of PHP 8.1 $GLOBALS can't be acces

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **4348** du fichier; voici le contexte :

ET) ? self::safe\_serialize($\_GET) : '') .

(isset($**\_COOKIE**) ? self::safe\_serialize($**\_COOKIE**) : '') .

// as of PHP 8.1 $GLOBALS can't be accessed by reference, which eliminate

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **5254** du fichier; voici le contexte :

session\_id($old\_session\_id);

session\_start();

ini\_set('session.use**\_cookie**s', $old\_use**\_cookie**s);

session\_cache\_limiter($old\_session\_cache\_limiter);

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **5273** du fichier; voici le contexte :

ession\_id);

session\_start();

ini\_set('session.use**\_cookie**s', $old\_use**\_cookie**s);

session\_cache\_limiter($old\_session\_cache\_limiter);

} else {

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\RSA\Formats\Keys\MSBLOB.php*(7.35K)(Date dernière modif. March 03 2024 04:14:58.)*a1de1d9b6003052b0874996e9777f8b4**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1696** du fichier; voici le contexte :
2. lueException('Key should be a string - not a ' . gettype($key));
3. }
4. $key = Strings::**base64\_decode**($key);
5. if (!is\_string($key)) {

throw new \UnexpectedValueException('Base64 dec

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Crypt\RSA\Formats\Keys\XML.php*(5.94K)(Date dernière modif. March 03 2024 04:14:58.)*feb14ff42e3bdd10e562cb758df8ed5d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2404** du fichier; voici le contexte :
2. emp->length) {
3. continue;
4. }
5. $value = new BigInteger(Strings::**base64\_decode**($temp->item(0)->nodeValue), 256);
6. switch ($key) {

case 'modulus':

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\File\ASN1.php*(59.19K)(Date dernière modif. March 03 2024 04:14:58.)*9c330e9177c634e14957fb126cd8323d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **58923** du fichier; voici le contexte :
2. +|-+[^-]+-+$#', '', $temp);
3. $temp = preg\_match('#^[a-zA-Z\d/+]\*={0,2}$#', $temp) ? Strings::**base64\_decode**($temp) : false;
4. return $temp != false ? $temp : $str;
5. }
6. /\*\*

\* DER-encode the

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\File\X509.php*(139.57K)(Date dernière modif. March 03 2024 04:14:58.)*3038c2a539e4adc9fcd4ed3b68f4cb29**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17649** du fichier; voici le contexte :
2. $cert['tbsCertificate']['subjectPublicKeyInfo'] = new Element(

**base64\_decode**(preg\_replace('#-.+-|[\r\n]#', '', $cert['tbsCertificate']['subjectPublicKeyInfo']['subjectPublicKey

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **84376** du fichier; voici le contexte :

$csr['certificationRequestInfo']['subjectPKInfo'] = new Element(

**base64\_decode**(preg\_replace('#-.+-|[\r\n]#', '', $csr['certificationRequestInfo']['subjectPKInfo']['subjectPublicK

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **86144** du fichier; voici le contexte :

|[ \r\n\\\]#', '', $spkac);

$temp = preg\_match('#^[a-zA-Z\d/+]\*={0,2}$#', $temp) ? Strings::**base64\_decode**($temp) : false;

if ($temp != false) {

$spkac = $temp;

}

$orig =

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **88094** du fichier; voici le contexte :

default:

$spkac['publicKeyAndChallenge']['spki'] = new Element(

**base64\_decode**(preg\_replace('#-.+-|[\r\n]#', '', $spkac['publicKeyAndChallenge']['spki']['subjectPublicKey']))

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **133952** du fichier; voici le contexte :

getPadding() & RSA::SIGNATURE\_PSS) ?

'PSS' :

'PKCS8';

$publicKey = **base64\_decode**(preg\_replace('#-.+-|[\r\n]#', '', $this->publicKey->toString($format)));

$decoded = ASN1::

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Math\BinaryField.php*(5.72K)(Date dernière modif. March 03 2024 04:14:58.)*a719268e25333c08ad7353a381b3eeef**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1364** du fichier; voici le contexte :
2. ecedented. in particular,
3. http://tools.ietf.org/html/rfc4253#section-6.1 (The Secure **Shell** (SSH) Transport Layer Protocol) says

"implementations SHOULD check that the packet l

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Net\SFTP.php*(117.07K)(Date dernière modif. March 03 2024 04:14:58.)*e470dd7a3aad2ae57faad6852f9f2570**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'hell**Trouvé en position **563** du fichier; voici le contexte :
2. exit('Login Failed');
3. \* }
4. \*
5. \* echo $sftp->pwd() . "\r\n";
6. \* $sftp->put('filename.ext', **'hell**o, world!');
7. \* print\_r($sftp->nlist());
8. \* ?>
9. \* </code>
10. \*

\* @author Jim Wigginton <terrafr

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\phpseclib\phpseclib\phpseclib\Net\SSH2.php*(187.71K)(Date dernière modif. March 03 2024 04:14:58.)*85a2b4686db0fc19c366dfb268ed3981**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **43650** du fichier; voici le contexte :
2. com', 'aes256-gcm@openssh.com']
3. ));
4. }
5. }
6. $client**\_cookie** = Random::string(16);

$kexinit\_payload\_client = pack('Ca\*', NET\_SSH2\_MSG\_KEXINIT, $client\_

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **43756** du fichier; voici le contexte :

e = Random::string(16);

$kexinit\_payload\_client = pack('Ca\*', NET\_SSH2\_MSG\_KEXINIT, $client**\_cookie**);

$kexinit\_payload\_client .= Strings::packSSH2(

'L10bN',

$kex\_algor

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **45142** du fichier; voici le contexte :

:shift($response, 1); // skip past the message number (it should be SSH\_MSG\_KEXINIT)

$server**\_cookie** = Strings::shift($response, 16);

list(

$this->kex\_algorithms,

$thi

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **1626** du fichier; voici le contexte :

clib3\Crypt\Rijndael;

use phpseclib3\Crypt\RSA;

use phpseclib3\Crypt\TripleDES; // Used to do Diffie**-Hell**man key exchange and DSA/RSA signature verification.

use phpseclib3\Crypt\Twofish;

use phpseclib3\Ex

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2743** du fichier; voici le contexte :

const MASK\_LOGIN\_REQ = 0x00000004;

const MASK\_LOGIN = 0x00000008;

const MASK\_**SHELL** = 0x00000010;

const MASK\_WINDOW\_ADJUST = 0x00000020;

/\*

\* Channel constants

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **3814** du fichier; voici le contexte :

channel\_packet()

\*/

const CHANNEL\_EXEC = 1; // PuTTy uses 0x100

const CHANNEL\_**SHELL** = 2;

const CHANNEL\_SUBSYSTEM = 3;

const CHANNEL\_AGENT\_FORWARD = 4;

const CH

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **6422** du fichier; voici le contexte :

\* @var string|false

\*/

private $kex\_algorithm = false;

/\*\*

\* Minimum Diffie**-Hell**man Group Bit Size in RFC 4419 Key Exchange Methods

\*

\* @see self::\_key\_exchange()

\*

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **6619** du fichier; voici le contexte :

\* @var int

\*/

private $kex\_dh\_group\_size\_min = 1536;

/\*\*

\* Preferred Diffie**-Hell**man Group Bit Size in RFC 4419 Key Exchange Methods

\*

\* @see self::\_key\_exchange()

\*

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **6820** du fichier; voici le contexte :

\* @var int

\*/

private $kex\_dh\_group\_size\_preferred = 2048;

/\*\*

\* Maximum Diffie**-Hell**man Group Bit Size in RFC 4419 Key Exchange Methods

\*

\* @see self::\_key\_exchange()

\*

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **28901** du fichier; voici le contexte :

61 => 'NET\_SSH2\_MSG\_USERAUTH\_INFO\_RESPONSE'],

// RFC 4419 - diffie**-hell**man-group-exchange-sha{1,256}

[30 => 'NET\_SSH2\_MSG\_KEXDH\_GEX\_REQUEST\_OLD',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **46350** du fichier; voici le contexte :

}

// we need to decide upon the symmetric encryption algorithms before we do the diffie**-hell**man key exchange

// we don't initialize any crypto-objects, yet - we do that, later. for no

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **46507** du fichier; voici le contexte :

crypto-objects, yet - we do that, later. for now, we need the lengths to make the

// diffie**-hell**man key exchange as fast as possible

$decrypt = self::array\_intersect\_first($s2c\_encryption\_

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **47474** du fichier; voici le contexte :

('No compatible client to server encryption algorithms found');

}

// through diffie**-hell**man key exchange a symmetric key is obtained

$this->kex\_algorithm = self::array\_intersect\_fi

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **50236** du fichier; voici le contexte :

n\_map[$compression\_algorithm\_out];

switch ($this->kex\_algorithm) {

case 'diffie**-hell**man-group15-sha512':

case 'diffie**-hell**man-group16-sha512':

case 'diffie**-hell**

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **50286** du fichier; voici le contexte :

($this->kex\_algorithm) {

case 'diffie**-hell**man-group15-sha512':

case 'diffie**-hell**man-group16-sha512':

case 'diffie**-hell**man-group17-sha512':

case 'diffie**-hell**

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **50336** du fichier; voici le contexte :

**-hell**man-group15-sha512':

case 'diffie**-hell**man-group16-sha512':

case 'diffie**-hell**man-group17-sha512':

case 'diffie**-hell**man-group18-sha512':

case 'ecdh-sha2-n

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **50386** du fichier; voici le contexte :

**-hell**man-group16-sha512':

case 'diffie**-hell**man-group17-sha512':

case 'diffie**-hell**man-group18-sha512':

case 'ecdh-sha2-nistp521':

$kexHash = new Hash('sha

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **50654** du fichier; voici le contexte :

384':

$kexHash = new Hash('sha384');

break;

case 'diffie**-hell**man-group-exchange-sha256':

case 'diffie**-hell**man-group14-sha256':

case 'ecdh

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **50711** du fichier; voici le contexte :

break;

case 'diffie**-hell**man-group-exchange-sha256':

case 'diffie**-hell**man-group14-sha256':

case 'ecdh-sha2-nistp256':

case 'curve25519-sha256@libs

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **51044** du fichier; voici le contexte :

default:

$kexHash = new Hash('sha1');

}

// Only relevant in diffie**-hell**man-group-exchange-sha{1,256}, otherwise empty.

$exchange\_hash\_rfc4419 = '';

if (s

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **51760** du fichier; voici le contexte :

'NET\_SSH2\_MSG\_KEX\_ECDH\_REPLY';

} else {

if (strpos($this->kex\_algorithm, 'diffie**-hell**man-group-exchange') === 0) {

$dh\_group\_sizes\_packed = pack(

'NN

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **99778** du fichier; voici le contexte :

n $this->get\_channel\_packet($channel, $skip\_extended);

}

/\*\*

\* Creates an interactive **shell**

\*

\* Returns bool(true) if the **shell** was opened.

\* Returns bool(false) if the **shell** w

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **99824** du fichier; voici le contexte :

tended);

}

/\*\*

\* Creates an interactive **shell**

\*

\* Returns bool(true) if the **shell** was opened.

\* Returns bool(false) if the **shell** was already open.

\*

\* @see self::isSh

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **99876** du fichier; voici le contexte :

e **shell**

\*

\* Returns bool(true) if the **shell** was opened.

\* Returns bool(false) if the **shell** was already open.

\*

\* @see self::isShellOpen()

\* @see self::read()

\* @see self:

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **99927** du fichier; voici le contexte :

ll was opened.

\* Returns bool(false) if the shell was already open.

\*

\* @see self::is**Shell**Open()

\* @see self::read()

\* @see self::write()

\* @return bool

\* @throws Insuffi

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **100228** du fichier; voici le contexte :

unexpected packets

\* @throws \RuntimeException on other errors

\*/

public function open**Shell**()

{

if (!$this->isAuthenticated()) {

throw new InsufficientSetupException('

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **100427** du fichier; voici le contexte :

tion('Operation disallowed prior to login()');

}

$this->open\_channel(self::CHANNEL\_**SHELL**);

$terminal\_modes = pack('C', NET\_SSH2\_TTY\_OP\_END);

$packet = Strings::packSSH2(

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **100646** du fichier; voici le contexte :

sbsN4s',

NET\_SSH2\_MSG\_CHANNEL\_REQUEST,

$this->server\_channels[self::CHANNEL\_**SHELL**],

'pty-req',

true, // want reply

$this->term,

$this

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **100958** du fichier; voici le contexte :

);

$this->send\_binary\_packet($packet);

$this->channel\_status[self::CHANNEL\_**SHELL**] = NET\_SSH2\_MSG\_CHANNEL\_REQUEST;

if (!$this->get\_channel\_packet(self::CHANNEL\_**SHELL**)) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **101051** du fichier; voici le contexte :

HANNEL\_**SHELL**] = NET\_SSH2\_MSG\_CHANNEL\_REQUEST;

if (!$this->get\_channel\_packet(self::CHANNEL\_**SHELL**)) {

throw new \RuntimeException('Unable to request pty');

}

$packet =

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **101286** du fichier; voici le contexte :

'CNsb',

NET\_SSH2\_MSG\_CHANNEL\_REQUEST,

$this->server\_channels[self::CHANNEL\_**SHELL**],

'shell',

true // want reply

);

$this->send\_binary\_packet(

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **101307** du fichier; voici le contexte :

NET\_SSH2\_MSG\_CHANNEL\_REQUEST,

$this->server\_channels[self::CHANNEL\_SHELL],

'**shell**',

true // want reply

);

$this->send\_binary\_packet($packet);

$r

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **101462** du fichier; voici le contexte :

$this->send\_binary\_packet($packet);

$response = $this->get\_channel\_packet(self::CHANNEL\_**SHELL**);

if ($response === false) {

throw new \RuntimeException('Unable to request she

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **101564** du fichier; voici le contexte :

ELL);

if ($response === false) {

throw new \RuntimeException('Unable to request **shell**');

}

$this->channel\_status[self::CHANNEL\_SHELL] = NET\_SSH2\_MSG\_CHANNEL\_DATA;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **101628** du fichier; voici le contexte :

RuntimeException('Unable to request shell');

}

$this->channel\_status[self::CHANNEL\_**SHELL**] = NET\_SSH2\_MSG\_CHANNEL\_DATA;

$this->channel\_id\_last\_interactive = self::CHANNEL\_**SHELL**;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **101724** du fichier; voici le contexte :

NEL\_**SHELL**] = NET\_SSH2\_MSG\_CHANNEL\_DATA;

$this->channel\_id\_last\_interactive = self::CHANNEL\_**SHELL**;

$this->bitmap |= self::MASK\_**SHELL**;

return true;

}

/\*\*

\* Return the

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **101768** du fichier; voici le contexte :

$this->channel\_id\_last\_interactive = self::CHANNEL\_**SHELL**;

$this->bitmap |= self::MASK\_**SHELL**;

return true;

}

/\*\*

\* Return the channel to be used with read(), write(), an

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **102596** du fichier; voici le contexte :

return self::CHANNEL\_EXEC;

default:

return self::CHANNEL\_**SHELL**;

}

}

/\*\*

\* Indicates the DATA status on the given channel

\*

\* @para

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **104274** du fichier; voici le contexte :

\_MSG\_CHANNEL\_OPEN;

return true;

}

/\*\*

\* Returns the output of an interactive **shell**

\*

\* Returns when there's a match for $expect, which can take the form of a string literal

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **104589** du fichier; voici le contexte :

open interactive channel will be selected, or, if there are

\* no open channels, an interactive **shell** will be created. If there are multiple open

\* interactive channels, a legacy behavior will app

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **104795** du fichier; voici le contexte :

y in which channel selection prioritizes

\* an active subsystem, the exec pty, and, lastly, the **shell**. If using multiple interactive

\* channels, callers are discouraged from relying on this legacy

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **105908** du fichier; voici le contexte :

a($channel) && empty($this->channel\_buffers[$channel])) {

if ($channel != self::CHANNEL\_**SHELL**) {

throw new InsufficientSetupException('Data is not available on channel');

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **106041** du fichier; voici le contexte :

w InsufficientSetupException('Data is not available on channel');

} elseif (!$this->open**Shell**()) {

throw new \RuntimeException('Unable to initiate an interactive shell session')

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **106131** du fichier; voici le contexte :

this->openShell()) {

throw new \RuntimeException('Unable to initiate an interactive **shell** session');

}

}

if ($mode == self::READ\_NEXT) {

return $thi

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **107095** du fichier; voici le contexte :

nteractiveBuffer .= $response;

}

}

/\*\*

\* Inputs a command into an interactive **shell**.

\*

\* If not specifying a channel, an open interactive channel will be selected, or, if th

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **107248** du fichier; voici le contexte :

open interactive channel will be selected, or, if there are

\* no open channels, an interactive **shell** will be created. If there are multiple open

\* interactive channels, a legacy behavior will app

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **107454** du fichier; voici le contexte :

y in which channel selection prioritizes

\* an active subsystem, the exec pty, and, lastly, the **shell**. If using multiple interactive

\* channels, callers are discouraged from relying on this legacy

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **108336** du fichier; voici le contexte :

if (!$this->is\_channel\_status\_data($channel)) {

if ($channel != self::CHANNEL\_**SHELL**) {

throw new InsufficientSetupException('Data is not available on channel');

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **108469** du fichier; voici le contexte :

w InsufficientSetupException('Data is not available on channel');

} elseif (!$this->open**Shell**()) {

throw new \RuntimeException('Unable to initiate an interactive shell session')

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **108559** du fichier; voici le contexte :

this->openShell()) {

throw new \RuntimeException('Unable to initiate an interactive **shell** session');

}

}

$this->send\_channel\_packet($channel, $cmd);

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **110864** du fichier; voici le contexte :

y in which channel selection

\* prioritizes an active subsystem, the exec pty, and, lastly, the **shell**. If using multiple

\* interactive channels, callers are discouraged from relying on this legacy

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **113992** du fichier; voici le contexte :

return (bool) ($this->bitmap & self::MASK\_LOGIN);

}

/\*\*

\* Is the interactive **shell** active?

\*

\* @return bool

\*/

public function isShellOpen()

{

return $

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **114063** du fichier; voici le contexte :

\*\*

\* Is the interactive shell active?

\*

\* @return bool

\*/

public function is**Shell**Open()

{

return $this->isInteractiveChannelOpen(self::CHANNEL\_SHELL);

}

/\*\*

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **114142** du fichier; voici le contexte :

public function isShellOpen()

{

return $this->isInteractiveChannelOpen(self::CHANNEL\_**SHELL**);

}

/\*\*

\* Is the exec pty active?

\*

\* @return bool

\*/

public funct

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **165410** du fichier; voici le contexte :

nel\_bitmap($client\_channel)

{

switch ($client\_channel) {

case self::CHANNEL\_**SHELL**:

// Shell status has been maintained in the bitmap for backwards

//

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **165436** du fichier; voici le contexte :

)

{

switch ($client\_channel) {

case self::CHANNEL\_SHELL:

// **Shell** status has been maintained in the bitmap for backwards

// compatibility sake, but

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **165617** du fichier; voici le contexte :

compatibility sake, but can be removed going forward

if ($this->bitmap & self::MASK\_**SHELL**) {

$this->bitmap &= ~self::MASK\_**SHELL**;

}

break;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **165675** du fichier; voici le contexte :

if ($this->bitmap & self::MASK\_**SHELL**) {

$this->bitmap &= ~self::MASK\_**SHELL**;

}

break;

}

}

/\*\*

\* Disconnect

\*

\*

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **172422** du fichier; voici le contexte :

n getSupportedKEXAlgorithms()

{

$kex\_algorithms = [

// Elliptic Curve Diffie**-Hell**man Key Agreement (ECDH) using

// Curve25519. See doc/curve25519-sha256@libssh.org.txt i

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **172824** du fichier; voici le contexte :

'ecdh-sha2-nistp384', // RFC 5656

'ecdh-sha2-nistp521', // RFC 5656

'diffie**-hell**man-group-exchange-sha256',// RFC 4419

'diffie**-hell**man-group-exchange-sha1', // RFC 441

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **172887** du fichier; voici le contexte :

21', // RFC 5656

'diffie**-hell**man-group-exchange-sha256',// RFC 4419

'diffie**-hell**man-group-exchange-sha1', // RFC 4419

// Diffie-Hellman Key Agreement (DH) using integ

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **172953** du fichier; voici le contexte :

6',// RFC 4419

'diffie-hellman-group-exchange-sha1', // RFC 4419

// Diffie**-Hell**man Key Agreement (DH) using integer modulo prime

// groups.

'diffie-hellman

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173050** du fichier; voici le contexte :

fie-Hellman Key Agreement (DH) using integer modulo prime

// groups.

'diffie**-hell**man-group14-sha256',

'diffie**-hell**man-group14-sha1', // REQUIRED

'diffie**-hell**

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173095** du fichier; voici le contexte :

modulo prime

// groups.

'diffie**-hell**man-group14-sha256',

'diffie**-hell**man-group14-sha1', // REQUIRED

'diffie**-hell**man-group15-sha512',

'diffie**-hell**

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173150** du fichier; voici le contexte :

**-hell**man-group14-sha256',

'diffie**-hell**man-group14-sha1', // REQUIRED

'diffie**-hell**man-group15-sha512',

'diffie**-hell**man-group16-sha512',

'diffie**-hell**man-group1

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173195** du fichier; voici le contexte :

**-hell**man-group14-sha1', // REQUIRED

'diffie**-hell**man-group15-sha512',

'diffie**-hell**man-group16-sha512',

'diffie**-hell**man-group17-sha512',

'diffie**-hell**man-group1

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173240** du fichier; voici le contexte :

'diffie**-hell**man-group15-sha512',

'diffie**-hell**man-group16-sha512',

'diffie**-hell**man-group17-sha512',

'diffie**-hell**man-group18-sha512',

'diffie**-hell**man-group

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173285** du fichier; voici le contexte :

'diffie**-hell**man-group16-sha512',

'diffie**-hell**man-group17-sha512',

'diffie**-hell**man-group18-sha512',

'diffie**-hell**man-group1-sha1', // REQUIRED

];

retu

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-hell**Trouvé en position **173331** du fichier; voici le contexte :

'diffie**-hell**man-group17-sha512',

'diffie**-hell**man-group18-sha512',

'diffie**-hell**man-group1-sha1', // REQUIRED

];

return $kex\_algorithms;

}

/\*\*

\* Retu

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\psr\http-message\src\ServerRequestInterface.php*(9.91K)(Date dernière modif. April 04 2023 13:50:52.)*90dbb3840dc0e0cfcaa929fb27b22e6d**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **526** du fichier; voici le contexte :
2. t, including:
3. \*
4. \* - The values represented in $\_SERVER.
5. \* - Any cookies provided (generally via $**\_COOKIE**)
6. \* - Query string arguments (generally via $\_GET, or as parsed via parse\_str())

\* - Upload files,

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **2247** du fichier; voici le contexte :

t by the client to the server.

\*

\* The data MUST be compatible with the structure of the $**\_COOKIE**

\* superglobal.

\*

\* @return array

\*/

public function getCookieParams();

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **2470** du fichier; voici le contexte :

rn an instance with the specified cookies.

\*

\* The data IS NOT REQUIRED to come from the $**\_COOKIE** superglobal, but MUST

\* be compatible with the structure of $**\_COOKIE**. Typically, this data wil

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **2544** du fichier; voici le contexte :

EQUIRED to come from the $**\_COOKIE** superglobal, but MUST

\* be compatible with the structure of $**\_COOKIE**. Typically, this data will

\* be injected at instantiation.

\*

\* This method MUST NOT

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\spomky-labs\cbor-php\src\Utils.php*(1.33K)(Date dernière modif. January 29 2024 22:33:48.)*da477ca6403864d3ede8876a6a676a9a**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **920** du fichier; voici le contexte :
2. toBase(10);
3. }
4. public static function decode(string $data): string
5. {
6. $decoded = **base64\_decode**(strtr($data, '-\_', '+/'), true);
7. if ($decoded === false) {

throw new InvalidArg

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki-framework\src\CryptoEncoding\PEM.php*(3.36K)(Date dernière modif. February 05 2024 22:37:46.)*ad457e5da0fce4d8385d7feeb43c0a04**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2291** du fichier; voici le contexte :
2. throw new UnexpectedValueException('Failed to decode PEM data.');
3. }
4. $data = **base64\_decode**($payload, true);
5. if ($data === false) {

throw new UnexpectedValueException('Fai

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki-framework\src\CryptoEncoding\PEMBundle.php*(3.58K)(Date dernière modif. February 05 2024 22:37:46.)*529112b140ed58d1c3f060d91cab28d5**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1493** du fichier; voici le contexte :
2. w UnexpectedValueException('Failed to decode PEM data.');
3. }
4. $data = **base64\_decode**($payload, true);
5. if ($data === false) {

throw new UnexpectedVal

×

1. D: \wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki- framework\src\CryptoTypes\AlgorithmIdentifier\Asymmetric\RFC8410XAlgorithmIdentifier.php*(1.13K)(Date dernière modif. February 05 2024 22:37:46.)*e96fb40a6f0fcc0c5486a14747ebd5de**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **843** du fichier; voici le contexte :
2. that subsystem and not propagated to the Internet.
3. \*/
4. /\*\*
5. \* Algorithm identifier for the Diffie**-Hell**man operations specified by RFC 8410.
6. \*
7. \* @see https://tools.ietf.org/html/rfc8410#section-3
8. \*/

a

×

1. D: \wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki- framework\src\CryptoTypes\AlgorithmIdentifier\Asymmetric\X25519AlgorithmIdentifier.php*(1.00K)(Date dernière modif. February 05 2024 22:37:46.)*842a94c29c106c348cf7e909e0ef0197**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **302** du fichier; voici le contexte :
2. ecificAlgorithmIdentifier;
3. use UnexpectedValueException;
4. /\*\*
5. \* Algorithm identifier for the Diffie**-Hell**man operation with curve25519.
6. \*
7. \* @see http://oid-info.com/get/1.3.101.110
8. \*/

final class X25519

×

1. D: \wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki- framework\src\CryptoTypes\AlgorithmIdentifier\Asymmetric\X448AlgorithmIdentifier.php*(0.99K)(Date dernière modif. February 05 2024 22:37:46.)*0cd872771f97c422eef1946339195a7e**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **-Hell**Trouvé en position **302** du fichier; voici le contexte :
2. ecificAlgorithmIdentifier;
3. use UnexpectedValueException;
4. /\*\*
5. \* Algorithm identifier for the Diffie**-Hell**man operation with curve448.
6. \*
7. \* @see http://oid-info.com/get/1.3.101.111
8. \*/

final class X448Algo

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki-framework\src\X501\ASN1\AttributeType.php*(17.54K)(Date dernière modif. February 05 2024 22:37:46.)*c5bac425665de2e68566a43aa6c8f173**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **10267** du fichier; voici le contexte :
2. ' => ['gecos'],
3. '1.3.6.1.1.1.1.3' => ['homeDirectory'],
4. '1.3.6.1.1.1.1.4' => ['login**Shell**'],
5. '1.3.6.1.1.1.1.5' => ['shadowLastChange'],

'1.3.6.1.1.1.1.6' => ['shadowMin'],

×

1. D: \wamp64\www\randophil.J5\libraries\vendor\spomky-labs\pki- framework\src\X509\Certificate\Extension\ExtendedKeyUsageExtension.php*(4.28K)(Date dernière modif. February 05 2024 22:37:46.)*0148e6a7b108946c4a03849a01ffea4f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **1927** du fichier; voici le contexte :
2. ;
3. final public const OID\_SIP\_DOMAIN = '1.3.6.1.5.5.7.3.20';
4. final public const OID\_SECURE\_**SHELL**\_CLIENT = '1.3.6.1.5.5.7.3.21';

final public const OID\_SECURE\_**SHELL**\_SERVER = '1.3.6.1.5.5.7.3.2

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **1999** du fichier; voici le contexte :

nal public const OID\_SECURE\_**SHELL**\_CLIENT = '1.3.6.1.5.5.7.3.21';

final public const OID\_SECURE\_**SHELL**\_SERVER = '1.3.6.1.5.5.7.3.22';

final public const OID\_SEND\_ROUTER = '1.3.6.1.5.5.7.3.23';

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Application.php*(46.25K)(Date dernière modif. February 22 2024 22:27:10.)*4399cfb6aa777040af03afe45a5352d9**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **32665** du fichier; voici le contexte :
2. nteraction', '-n'], true)) {
3. $input->setInteractive(false);
4. }
5. switch ($**shell**Verbosity = (int) getenv('SHELL\_VERBOSITY')) {
6. case -1:

$output->setVerb

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **32696** du fichier; voici le contexte :

$input->setInteractive(false);

}

switch ($shellVerbosity = (int) getenv('**SHELL**\_VERBOSITY')) {

case -1:

$output->setVerbosity(OutputInterface::VERBOSIT

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **33229** du fichier; voici le contexte :

ity(OutputInterface::VERBOSITY\_DEBUG);

break;

default:

$**shell**Verbosity = 0;

break;

}

if (true === $input->hasParameterOption(['-

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **33441** du fichier; voici le contexte :

, '-q'], true)) {

$output->setVerbosity(OutputInterface::VERBOSITY\_QUIET);

$**shell**Verbosity = -1;

} else {

if ($input->hasParameterOption('-vvv', true) || $input-

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **33742** du fichier; voici le contexte :

true)) {

$output->setVerbosity(OutputInterface::VERBOSITY\_DEBUG);

$**shell**Verbosity = 3;

} elseif ($input->hasParameterOption('-vv', true) || $input->hasParameter

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **34037** du fichier; voici le contexte :

{

$output->setVerbosity(OutputInterface::VERBOSITY\_VERY\_VERBOSE);

$**shell**Verbosity = 2;

} elseif ($input->hasParameterOption('-v', true) || $input->hasParameterO

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **34369** du fichier; voici le contexte :

rue)) {

$output->setVerbosity(OutputInterface::VERBOSITY\_VERBOSE);

$**shell**Verbosity = 1;

}

}

if (-1 === $**shell**Verbosity) {

$input->se

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **34434** du fichier; voici le contexte :

RBOSITY\_VERBOSE);

$**shell**Verbosity = 1;

}

}

if (-1 === $**shell**Verbosity) {

$input->setInteractive(false);

}

if (\function\_exists('put

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **34569** du fichier; voici le contexte :

t->setInteractive(false);

}

if (\function\_exists('putenv')) {

@putenv('**SHELL**\_VERBOSITY='.$shellVerbosity);

}

$\_ENV['**SHELL**\_VERBOSITY'] = $shellVerbosity;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **34588** du fichier; voici le contexte :

alse);

}

if (\function\_exists('putenv')) {

@putenv('SHELL\_VERBOSITY='.$**shell**Verbosity);

}

$\_ENV['SHELL\_VERBOSITY'] = $**shell**Verbosity;

$\_SERVER['SHELL\_VE

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **34630** du fichier; voici le contexte :

ists('putenv')) {

@putenv('**SHELL**\_VERBOSITY='.$shellVerbosity);

}

$\_ENV['**SHELL**\_VERBOSITY'] = $shellVerbosity;

$\_SERVER['**SHELL**\_VERBOSITY'] = $shellVerbosity;

}

/\*

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **34651** du fichier; voici le contexte :

@putenv('SHELL\_VERBOSITY='.$**shell**Verbosity);

}

$\_ENV['SHELL\_VERBOSITY'] = $**shell**Verbosity;

$\_SERVER['SHELL\_VERBOSITY'] = $**shell**Verbosity;

}

/\*\*

\* Runs the cur

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **34685** du fichier; voici le contexte :

'.$shellVerbosity);

}

$\_ENV['**SHELL**\_VERBOSITY'] = $shellVerbosity;

$\_SERVER['**SHELL**\_VERBOSITY'] = $shellVerbosity;

}

/\*\*

\* Runs the current command.

\*

\* If an

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **34706** du fichier; voici le contexte :

}

$\_ENV['SHELL\_VERBOSITY'] = $**shell**Verbosity;

$\_SERVER['SHELL\_VERBOSITY'] = $**shell**Verbosity;

}

/\*\*

\* Runs the current command.

\*

\* If an event dispatcher has

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **35848** du fichier; voici le contexte :

tive.');

}

if (Terminal::hasSttyAvailable()) {

$sttyMode = **shell\_exec**('stty -g');

foreach ([\SIGINT, \SIGTERM] as $signal) {

$this->

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **36008** du fichier; voici le contexte :

SIGTERM] as $signal) {

$this->signalRegistry->register($signal, static fn () => **shell\_exec**('stty '.$sttyMode));

}

}

if ($this->dispatcher) {

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Command\CompleteCommand.php*(9.05K)(Date dernière modif. February 22 2024 22:27:10.)*798b17ff52da7e5ca95db2a30dbd073b**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1074** du fichier; voici le contexte :
2. mfony\Component\Console\Output\OutputInterface;
3. /\*\*
4. \* Responsible for providing the values to the **shell** completion.
5. \*
6. \* @author Wouter de Jong <wouter@wouterj.nl>
7. \*/

#[AsCommand(name: '|\_complete', de

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1219** du fichier; voici le contexte :

g <wouter@wouterj.nl>

\*/

#[AsCommand(name: '|\_complete', description: 'Internal command to provide **shell** completion suggestions')]

final class CompleteCommand extends Command

{

public const COMPLETION

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1574** du fichier; voici le contexte :

d since Symfony 6.1

\*/

protected static $defaultDescription = 'Internal command to provide **shell** completion suggestions';

private array $completionOutputs;

private bool $isDebug = false;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1823** du fichier; voici le contexte :

string<CompletionOutputInterface>> $completionOutputs A list of additional completion outputs, with **shell** name as key and FQCN as value

\*/

public function \_\_construct(array $completionOutputs = []

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2380** du fichier; voici le contexte :

uct();

}

protected function configure(): void

{

$this

->addOption('**shell**', 's', InputOption::VALUE\_REQUIRED, 'The **shell** type ("'.implode('", "', array\_keys($this->completio

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2427** du fichier; voici le contexte :

): void

{

$this

->addOption('**shell**', 's', InputOption::VALUE\_REQUIRED, 'The **shell** type ("'.implode('", "', array\_keys($this->completionOutputs)).'")')

->addOption('input

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3372** du fichier; voici le contexte :

terface $output): int

{

try {

// "symfony" must be kept for compat with the **shell** scripts generated by Symfony Console 5.4 - 6.1

$version = $input->getOption('symfony')

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3986** du fichier; voici le contexte :

gain by using the "completion" command.');

return 126;

}

$**shell** = $input->getOption('**shell**');

if (!$**shell**) {

throw new \RuntimeExceptio

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4013** du fichier; voici le contexte :

on" command.');

return 126;

}

$**shell** = $input->getOption('**shell**');

if (!$**shell**) {

throw new \RuntimeException('The "--**shell**" option mus

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4040** du fichier; voici le contexte :

return 126;

}

$**shell** = $input->getOption('**shell**');

if (!$**shell**) {

throw new \RuntimeException('The "--**shell**" option must be set.');

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4101** du fichier; voici le contexte :

>getOption('**shell**');

if (!$**shell**) {

throw new \RuntimeException('The "--**shell**" option must be set.');

}

if (!$completionOutput = $this->completionOutput

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4209** du fichier; voici le contexte :

ption must be set.');

}

if (!$completionOutput = $this->completionOutputs[$**shell**] ?? false) {

throw new \RuntimeException(sprintf('Shell completion is not supported

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **4281** du fichier; voici le contexte :

= $this->completionOutputs[$shell] ?? false) {

throw new \RuntimeException(sprintf('**Shell** completion is not supported for your shell: "%s" (supported: "%s").', $shell, implode('", "', array

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4324** du fichier; voici le contexte :

) {

throw new \RuntimeException(sprintf('Shell completion is not supported for your **shell**: "%s" (supported: "%s").', $**shell**, implode('", "', array\_keys($this->completionOutputs))));

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4358** du fichier; voici le contexte :

timeException(sprintf('Shell completion is not supported for your **shell**: "%s" (supported: "%s").', $**shell**, implode('", "', array\_keys($this->completionOutputs))));

}

$completionInp

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Command\DumpCompletionCommand.php*(5.31K)(Date dernière modif. February 22 2024 22:27:10.)*43255e9bf65b0392bca75e82f24df8af**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **693** du fichier; voici le contexte :
2. terface;
3. use Symfony\Component\Process\Process;
4. /\*\*
5. \* Dumps the completion script for the current **shell**.
6. \*
7. \* @author Wouter de Jong <wouter@wouterj.nl>
8. \*/

#[AsCommand(name: 'completion', description:

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **808** du fichier; voici le contexte :

uthor Wouter de Jong <wouter@wouterj.nl>

\*/

#[AsCommand(name: 'completion', description: 'Dump the **shell** completion script')]

final class DumpCompletionCommand extends Command

{

/\*\*

\* @deprecated

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1097** du fichier; voici le contexte :

\*

\* @deprecated since Symfony 6.1

\*/

protected static $defaultDescription = 'Dump the **shell** completion script';

private array $supportedShells;

protected function configure(): void

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1152** du fichier; voici le contexte :

ected static $defaultDescription = 'Dump the shell completion script';

private array $supported**Shell**s;

protected function configure(): void

{

$fullCommand = $\_SERVER['PHP\_SELF'];

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1374** du fichier; voici le contexte :

= basename($fullCommand);

$fullCommand = @realpath($fullCommand) ?: $fullCommand;

$**shell** = $this->guessShell();

[$rcFile, $completionFile] = match ($**shell**) {

'fish' =>

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1394** du fichier; voici le contexte :

and);

$fullCommand = @realpath($fullCommand) ?: $fullCommand;

$shell = $this->guess**Shell**();

[$rcFile, $completionFile] = match ($shell) {

'fish' => ['~/.config/fish/con

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1448** du fichier; voici le contexte :

: $fullCommand;

$**shell** = $this->guessShell();

[$rcFile, $completionFile] = match ($**shell**) {

'fish' => ['~/.config/fish/config.fish', "/etc/fish/completions/$commandName.fish"],

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1724** du fichier; voici le contexte :

default => ['~/.bashrc', "/etc/bash\_completion.d/$commandName"],

};

$supported**Shell**s = implode(', ', $this->getSupported**Shell**s());

$this

->setHelp(<<<EOH

The <inf

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1766** du fichier; voici le contexte :

ompletion.d/$commandName"],

};

$supported**Shell**s = implode(', ', $this->getSupported**Shell**s());

$this

->setHelp(<<<EOH

The <info>%command.name%</> command dumps the shel

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1867** du fichier; voici le contexte :

hells());

$this

->setHelp(<<<EOH

The <info>%command.name%</> command dumps the **shell** completion script required

to use **shell** autocompletion (currently, {$supportedShells} completion ar

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1907** du fichier; voici le contexte :

etHelp(<<<EOH

The <info>%command.name%</> command dumps the **shell** completion script required

to use **shell** autocompletion (currently, {$supportedShells} completion are supported).

<comment>Static installat

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1951** du fichier; voici le contexte :

mmand dumps the shell completion script required

to use shell autocompletion (currently, {$supported**Shell**s} completion are supported).

<comment>Static installation

-------------------</>

Dump the script

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2101** du fichier; voici le contexte :

c installation

-------------------</>

Dump the script to a global completion file and restart your **shell**:

<info>%command.full\_name% {$**shell**} | sudo tee {$completionFile}</>

Or dump the script to a l

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2141** du fichier; voici le contexte :

ump the script to a global completion file and restart your **shell**:

<info>%command.full\_name% {$**shell**} | sudo tee {$completionFile}</>

Or dump the script to a local file and source it:

<info>%com

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2264** du fichier; voici le contexte :

pletionFile}</>

Or dump the script to a local file and source it:

<info>%command.full\_name% {$**shell**} > completion.sh</>

<comment># source the file whenever you use the project</>

<info>sourc

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2588** du fichier; voici le contexte :

ompletion.sh</>

<comment>Dynamic installation

--------------------</>

Add this to the end of your **shell** configuration file (e.g. <info>"{$rcFile}"</>):

<info>eval "$({$fullCommand} completion {$shel

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2689** du fichier; voici le contexte :

hell configuration file (e.g. <info>"{$rcFile}"</>):

<info>eval "$({$fullCommand} completion {$**shell**})"</>

EOH

)

->addArgument('**shell**', InputArgument::OPTIONAL, 'The **shell** type

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2746** du fichier; voici le contexte :

<info>eval "$({$fullCommand} completion {$**shell**})"</>

EOH

)

->addArgument('**shell**', InputArgument::OPTIONAL, 'The **shell** type (e.g. "bash"), the value of the "$SHELL" env var will be

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2784** du fichier; voici le contexte :

on {$**shell**})"</>

EOH

)

->addArgument('**shell**', InputArgument::OPTIONAL, 'The **shell** type (e.g. "bash"), the value of the "$SHELL" env var will be used if this is not given', null, $th

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2829** du fichier; voici le contexte :

->addArgument('shell', InputArgument::OPTIONAL, 'The shell type (e.g. "bash"), the value of the "$**SHELL**" env var will be used if this is not given', null, $this->getSupportedShells(...))

->ad

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **2905** du fichier; voici le contexte :

h"), the value of the "$SHELL" env var will be used if this is not given', null, $this->getSupported**Shell**s(...))

->addOption('debug', null, InputOption::VALUE\_NONE, 'Tail the completion debug l

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3318** du fichier; voici le contexte :

$this->tailDebugLog($commandName, $output);

return 0;

}

$**shell** = $input->getArgument('**shell**') ?? self::guessShell();

$completionFile = \_\_DIR\_\_.'/../Resour

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3347** du fichier; voici le contexte :

Log($commandName, $output);

return 0;

}

$**shell** = $input->getArgument('**shell**') ?? self::guessShell();

$completionFile = \_\_DIR\_\_.'/../Resources/completion.'.$**shell**;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **3369** du fichier; voici le contexte :

put);

return 0;

}

$shell = $input->getArgument('shell') ?? self::guess**Shell**();

$completionFile = \_\_DIR\_\_.'/../Resources/completion.'.$shell;

if (!file\_exists($

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3441** du fichier; voici le contexte :

ment('**shell**') ?? self::guessShell();

$completionFile = \_\_DIR\_\_.'/../Resources/completion.'.$**shell**;

if (!file\_exists($completionFile)) {

$supportedShells = $this->getSupportedShe

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **3515** du fichier; voici le contexte :

./Resources/completion.'.$shell;

if (!file\_exists($completionFile)) {

$supported**Shell**s = $this->getSupported**Shell**s();

if ($output instanceof ConsoleOutputInterface) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **3543** du fichier; voici le contexte :

ell;

if (!file\_exists($completionFile)) {

$supported**Shell**s = $this->getSupported**Shell**s();

if ($output instanceof ConsoleOutputInterface) {

$output = $output

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3699** du fichier; voici le contexte :

putInterface) {

$output = $output->getErrorOutput();

}

if ($**shell**) {

$output->writeln(sprintf('<error>Detected **shell** "%s", which is not supported by

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3766** du fichier; voici le contexte :

;

}

if ($**shell**) {

$output->writeln(sprintf('<error>Detected **shell** "%s", which is not supported by Symfony **shell** completion (supported **shell**s: "%s").</>', $**shell**, imp

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3812** du fichier; voici le contexte :

$output->writeln(sprintf('<error>Detected **shell** "%s", which is not supported by Symfony **shell** completion (supported **shell**s: "%s").</>', $**shell**, implode('", "', $supportedShells)));

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3840** du fichier; voici le contexte :

(sprintf('<error>Detected **shell** "%s", which is not supported by Symfony **shell** completion (supported **shell**s: "%s").</>', $**shell**, implode('", "', $supportedShells)));

} else {

$ou

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **3861** du fichier; voici le contexte :

cted **shell** "%s", which is not supported by Symfony **shell** completion (supported **shell**s: "%s").</>', $**shell**, implode('", "', $supportedShells)));

} else {

$output->writeln(sprintf

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **3894** du fichier; voici le contexte :

ported by Symfony shell completion (supported shells: "%s").</>', $shell, implode('", "', $supported**Shell**s)));

} else {

$output->writeln(sprintf('<error>**Shell** not detected, Symf

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **3975** du fichier; voici le contexte :

('", "', $supported**Shell**s)));

} else {

$output->writeln(sprintf('<error>**Shell** not detected, Symfony shell completion only supports "%s").</>', implode('", "', $supported**Shell**s))

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4003** du fichier; voici le contexte :

;

} else {

$output->writeln(sprintf('<error>Shell not detected, Symfony **shell** completion only supports "%s").</>', implode('", "', $supportedShells)));

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **4072** du fichier; voici le contexte :

or>**Shell** not detected, Symfony shell completion only supports "%s").</>', implode('", "', $supported**Shell**s)));

}

return 2;

}

$output->write(str\_replace(['{{ COMMAN

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **4361** du fichier; voici le contexte :

], file\_get\_contents($completionFile)));

return 0;

}

private static function guess**Shell**(): string

{

return basename($\_SERVER['SHELL'] ?? '');

}

private function tailD

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **4417** du fichier; voici le contexte :

0;

}

private static function guessShell(): string

{

return basename($\_SERVER['**SHELL**'] ?? '');

}

private function tailDebugLog(string $commandName, OutputInterface $output): v

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **4971** du fichier; voici le contexte :

$line);

});

}

/\*\*

\* @return string[]

\*/

private function getSupported**Shell**s(): array

{

if (isset($this->supported**Shell**s)) {

return $this->supportedShe

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **5027** du fichier; voici le contexte :

[]

\*/

private function getSupported**Shell**s(): array

{

if (isset($this->supported**Shell**s)) {

return $this->supported**Shell**s;

}

$shells = [];

foreach (

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **5073** du fichier; voici le contexte :

ells(): array

{

if (isset($this->supported**Shell**s)) {

return $this->supported**Shell**s;

}

$shells = [];

foreach (new \DirectoryIterator(\_\_DIR\_\_.'/../Resources/

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **5101** du fichier; voici le contexte :

if (isset($this->supportedShells)) {

return $this->supportedShells;

}

$**shell**s = [];

foreach (new \DirectoryIterator(\_\_DIR\_\_.'/../Resources/') as $file) {

i

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **5301** du fichier; voici le contexte :

if (str\_starts\_with($file->getBasename(), 'completion.') && $file->isFile()) {

$**shell**s[] = $file->getExtension();

}

}

sort($**shell**s);

return $this->s

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **5373** du fichier; voici le contexte :

sFile()) {

$**shell**s[] = $file->getExtension();

}

}

sort($**shell**s);

return $this->supportedShells = $**shell**s;

}

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **5414** du fichier; voici le contexte :

ile->getExtension();

}

}

sort($shells);

return $this->supported**Shell**s = $shells;

}

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **5424** du fichier; voici le contexte :

tension();

}

}

sort($**shell**s);

return $this->supportedShells = $**shell**s;

}

}

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Completion\CompletionInput.php*(7.95K)(Date dernière modif. February 22 2024 22:27:10.)*7faf1feda55f1c2c94a7eaf4a1cbd1b4**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **527** du fichier; voici le contexte :
2. \InputDefinition;
3. use Symfony\Component\Console\Input\InputOption;
4. /\*\*
5. \* An input specialized for **shell** completion.
6. \*
7. \* This input allows unfinished option names or values and exposes what kind of

\* c

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **1226** du fichier; voici le contexte :

ue = '';

/\*\*

\* Converts a terminal string into tokens.

\*

\* This is required for **shell** completions without COMP\_WORDS support.

\*/

public static function fromString(string $input

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Completion\Output\CompletionOutputInterface.php*(704.00B)(Date dernière modif. February 22 2024 22:27:10.)*a72fff5262bf4da279b7bfe73fb64c02**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **499** du fichier; voici le contexte :
2. utInterface;
3. /\*\*
4. \* Transforms the {@see CompletionSuggestions} object into output readable by the **shell** completion.
5. \*
6. \* @author Wouter de Jong <wouter@wouterj.nl>
7. \*/

interface CompletionOutputInterfac

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Cursor.php*(3.92K)(Date dernière modif. February 22 2024 22:27:10.)*da88cdda0624a13951bf7a3ad634249d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **3712** du fichier; voici le contexte :
2. RY\_SEPARATOR && stream\_isatty(\STDOUT)) {
3. return [1, 1];
4. }
5. $sttyMode = **shell\_exec**('stty -g');
6. **shell\_exec**('stty -icanon -echo');

@fwrite($this->input, "\033[6n");

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **3743** du fichier; voici le contexte :

STDOUT)) {

return [1, 1];

}

$sttyMode = **shell\_exec**('stty -g');

**shell\_exec**('stty -icanon -echo');

@fwrite($this->input, "\033[6n");

$code = trim(fread($this

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **3879** du fichier; voici le contexte :

@fwrite($this->input, "\033[6n");

$code = trim(fread($this->input, 1024));

**shell\_exec**(sprintf('stty %s', $sttyMode));

sscanf($code, "\033[%d;%dR", $row, $col);

return

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Helper\QuestionHelper.php*(18.93K)(Date dernière modif. February 22 2024 22:27:10.)*a9ff127c599c33461629e74e9bafff94**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **7819** du fichier; voici le contexte :
2. $matches = $autocomplete($ret);
3. $numMatches = \count($matches);
4. $sttyMode = **shell\_exec**('stty -g');

$isStdin = 'php://stdin' === (stream\_get\_meta\_data($inputStream)['uri'] ?? null

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **8086** du fichier; voici le contexte :

// Disable icanon (so we can fread each keypress) and echo (we'll do echoing here instead)

**shell\_exec**('stty -icanon -echo');

// Add highlighted text style

$output->getFormatter()->setS

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **8771** du fichier; voici le contexte :

(false === $c || ('' === $ret && '' === $c && null === $question->getDefault())) {

**shell\_exec**('stty '.$sttyMode);

throw new MissingInputException('Aborted.');

} else

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **12865** du fichier; voici le contexte :

torePosition();

}

}

// Reset stty so it behaves normally again

**shell\_exec**('stty '.$sttyMode);

return $fullChoice;

}

private function mostRecentlyEnteredVal

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **14136** du fichier; voici le contexte :

copy($exe, $tmpExe);

$exe = $tmpExe;

}

$sExec = **shell\_exec**('"'.$exe.'"');

$value = $trimmable ? rtrim($sExec) : $sExec;

$output->write

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **14458** du fichier; voici le contexte :

alue;

}

if (self::$stty && Terminal::hasSttyAvailable()) {

$sttyMode = **shell\_exec**('stty -g');

**shell\_exec**('stty -echo');

} elseif ($this->isInteractiveInput($inpu

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **14493** du fichier; voici le contexte :

$stty && Terminal::hasSttyAvailable()) {

$sttyMode = **shell\_exec**('stty -g');

**shell\_exec**('stty -echo');

} elseif ($this->isInteractiveInput($inputStream)) {

throw new R

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **14928** du fichier; voici le contexte :

tErrorOutput() : $output;

$errOutput->warning('The value was possibly truncated by your **shell** or terminal emulator');

}

if (self::$stty && Terminal::hasSttyAvailable()) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **15040** du fichier; voici le contexte :

minal emulator');

}

if (self::$stty && Terminal::hasSttyAvailable()) {

**shell\_exec**('stty '.$sttyMode);

}

if (false === $value) {

throw new MissingInputEx

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Input\Input.php*(5.07K)(Date dernière modif. February 22 2024 22:27:10.)*23c33697fdd269e72511cf8fbcd55e5f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4717** du fichier; voici le contexte :
2. name) || $this->definition->hasNegation($name);
3. }
4. /\*\*
5. \* Escapes a token through escape**shell**arg if it contains unsafe chars.
6. \*/

public function escapeToken(string $token): string

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **4889** du fichier; voici le contexte :

Token(string $token): string

{

return preg\_match('{^[\w-]+$}', $token) ? $token : escape**shell**arg($token);

}

/\*\*

\* @param resource $stream

\*

\* @return void

\*/

pu

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Terminal.php*(6.89K)(Date dernière modif. February 22 2024 22:27:10.)*bfe125165da2033a3147b5be8f452c75**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **3113** du fichier; voici le contexte :
2. if (null !== self::$stty) {
3. return self::$stty;
4. }
5. // skip check if **shell\_exec** function is disabled
6. if (!\function\_exists('**shell\_exec**')) {

return false;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **3176** du fichier; voici le contexte :

}

// skip check if **shell\_exec** function is disabled

if (!\function\_exists('**shell\_exec**')) {

return false;

}

return self::$stty = (bool) **shell\_exec**('stty 2> '

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell\_exec**Trouvé en position **3265** du fichier; voici le contexte :

on\_exists('**shell\_exec**')) {

return false;

}

return self::$stty = (bool) **shell\_exec**('stty 2> '.('\\' === \DIRECTORY\_SEPARATOR ? 'NUL' : '/dev/null'));

}

private static functi

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\console\Tester\ApplicationTester.php*(2.61K)(Date dernière modif. February 22 2024 22:27:10.)*43067d833759f2a3e1efdce18e56efdb**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **1362** du fichier; voici le contexte :
2. xit code
3. \*/
4. public function run(array $input, array $options = []): int
5. {
6. $prev**Shell**Verbosity = getenv('SHELL\_VERBOSITY');
7. try {

$this->input = new ArrayInput($inp

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **1387** du fichier; voici le contexte :

ic function run(array $input, array $options = []): int

{

$prevShellVerbosity = getenv('**SHELL**\_VERBOSITY');

try {

$this->input = new ArrayInput($input);

if (isse

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **1902** du fichier; voici le contexte :

atusCode = $this->application->run($this->input, $this->output);

} finally {

// **SHELL**\_VERBOSITY is set by Application::configureIO so we need to unset/reset it

// to its pre

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **2113** du fichier; voici le contexte :

value to avoid one test's verbosity to spread to the following tests

if (false === $prev**Shell**Verbosity) {

if (\function\_exists('putenv')) {

@putenv('SHELL\_VE

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2210** du fichier; voici le contexte :

revShellVerbosity) {

if (\function\_exists('putenv')) {

@putenv('**SHELL**\_VERBOSITY');

}

unset($\_ENV['**SHELL**\_VERBOSITY']);

uns

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2276** du fichier; voici le contexte :

)) {

@putenv('**SHELL**\_VERBOSITY');

}

unset($\_ENV['**SHELL**\_VERBOSITY']);

unset($\_SERVER['**SHELL**\_VERBOSITY']);

} else {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2328** du fichier; voici le contexte :

}

unset($\_ENV['**SHELL**\_VERBOSITY']);

unset($\_SERVER['**SHELL**\_VERBOSITY']);

} else {

if (\function\_exists('putenv')) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2448** du fichier; voici le contexte :

} else {

if (\function\_exists('putenv')) {

@putenv('**SHELL**\_VERBOSITY='.$prevShellVerbosity);

}

$\_ENV['**SHELL**\_VERBOSITY'] = $pre

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **2471** du fichier; voici le contexte :

if (\function\_exists('putenv')) {

@putenv('SHELL\_VERBOSITY='.$prev**Shell**Verbosity);

}

$\_ENV['SHELL\_VERBOSITY'] = $prev**Shell**Verbosity;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2529** du fichier; voici le contexte :

@putenv('**SHELL**\_VERBOSITY='.$prevShellVerbosity);

}

$\_ENV['**SHELL**\_VERBOSITY'] = $prevShellVerbosity;

$\_SERVER['**SHELL**\_VERBOSITY'] = $prevShellVerbosit

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **2554** du fichier; voici le contexte :

VERBOSITY='.$prev**Shell**Verbosity);

}

$\_ENV['SHELL\_VERBOSITY'] = $prev**Shell**Verbosity;

$\_SERVER['SHELL\_VERBOSITY'] = $prev**Shell**Verbosity;

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **2596** du fichier; voici le contexte :

}

$\_ENV['**SHELL**\_VERBOSITY'] = $prevShellVerbosity;

$\_SERVER['**SHELL**\_VERBOSITY'] = $prevShellVerbosity;

}

}

}

}

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **2621** du fichier; voici le contexte :

$\_ENV['SHELL\_VERBOSITY'] = $prev**Shell**Verbosity;

$\_SERVER['SHELL\_VERBOSITY'] = $prev**Shell**Verbosity;

}

}

}

}

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\http-client\CurlHttpClient.php*(23.02K)(Date dernière modif. March 02 2024 14:45:30.)*8f27958b15d0665407c53a9e7740d857**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **4470** du fichier; voici le contexte :
2. OPT\_MAXREDIRS => 0 < $options['max\_redirects'] ? $options['max\_redirects'] : 0,
3. \CURLOPT**\_COOKIE**FILE => '', // Keep track of cookies during redirects

\CURLOPT\_TIMEOUT => 0,

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **22319** du fichier; voici le contexte :

AL\_CACHE,

\CURLOPT\_PROTOCOLS,

\CURLOPT\_REDIR\_PROTOCOLS,

\CURLOPT**\_COOKIE**FILE,

\CURLINFO\_REDIRECT\_COUNT,

];

if (\defined('CURLOPT\_HTTP09\_ALLOWED

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\http-client\DataCollector\HttpClientDataCollector.php*(8.31K)(Date dernière modif. March 02 2024 14:45:30.)*57ac65c26265e4e33d4ff918aa7483ef**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **6106** du fichier; voici le contexte :
2. t => $ip) {
3. if (null !== $ip) {
4. $command[] = '--resolve '.escape**shell**arg("$host:$port:$ip");
5. }
6. }
7. }
8. $dataArg = [];

i

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **7835** du fichier; voici le contexte :

mand[] = sprintf('--request %s', $match[1]);

$command[] = sprintf('--url %s', escape**shell**arg($url));

continue;

}

$command[] = '--header '.escapeshel

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **7936** du fichier; voici le contexte :

hellarg($url));

continue;

}

$command[] = '--header '.escape**shell**arg($line);

}

if (null !== $dataArg) {

$command[] = $dataArg;

}

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\http-client\Internal\AmpListener.php*(5.34K)(Date dernière modif. March 02 2024 14:45:30.)*ab76db70d8a47da0824b2be68933093f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3056** du fichier; voici le contexte :
2. in)['key'];
3. $pin = \array\_slice(explode("\n", $pin), 1, -2);
4. $pin = **base64\_decode**(implode('', $pin));

$pin = base64\_encode(hash('sha256', $pin, true));

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\http-client\Test\HarFileResponseFactory.php*(3.20K)(Date dernière modif. March 02 2024 14:45:30.)*f0e2a6374e41a8db0d00c20dc28a0e26**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3066** du fichier; voici le contexte :
2. ncoding = $content['encoding'] ?? null;
3. return match ($encoding) {
4. 'base64' => **base64\_decode**($text),
5. null => $text,

default => throw new \InvalidArgumentException(sprin

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\http-client-contracts\Test\HttpClientTestCase.php*(37.02K)(Date dernière modif. July 31 2023 00:28:32.)*d2d956a631bce1f34706ecd53a30204e**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzdecode**Trouvé en position **36550** du fichier; voici le contexte :
2. $response->getContent();
3. $this->assertSame("\x1F", $body[0]);
4. $body = json\_decode(**gzdecode**($body), true);
5. $this->assertSame('gzip', $body['HTTP\_ACCEPT\_ENCODING']);
6. }

/\*\*

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\polyfill-iconv\Iconv.php*(22.09K)(Date dernière modif. January 29 2024 22:11:04.)*32bdaa9ad7f09f0116fb5de0f1fc291e**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9752** du fichier; voici le contexte :
2. $d = false;
3. } elseif ('B' === strtoupper($str[$i + 1])) {
4. $d = **base64\_decode**($str[$i + 2]);
5. } else {

$d = rawurldecode(strtr(str\_replace('%', '%25',

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\polyfill-mbstring\Mbstring.php*(31.41K)(Date dernière modif. January 29 2024 22:11:04.)*d4d2803c2520677145e1140eece7a1f2**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4759** du fichier; voici le contexte :
2. oding = self::getEncoding($toEncoding);
3. if ('BASE64' === $fromEncoding) {
4. $s = **base64\_decode**($s);
5. $fromEncoding = $toEncoding;
6. }

if ('BASE64' === $toEncoding) {

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\validator\Constraints\CssColorValidator.php*(5.34K)(Date dernière modif. February 22 2024 22:27:10.)*caf4b803afb27f729e684adfe568bead**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **2580** du fichier; voici le contexte :

|peru|pink|plum|powderblue|purple|red|rosybrown|royalblue|saddlebrown|salmon|sandybrown|seagreen|sea**shell**|sienna|silver|skyblue|slateblue|slategray|slategrey|snow|springgreen|steelblue|tan|teal|thistle|tom

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\validator\Constraints\IbanValidator.php*(12.13K)(Date dernière modif. February 22 2024 22:27:10.)*f345c6443e91089e72e1d4f830b88c3d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **chell**Trouvé en position **7319** du fichier; voici le contexte :
2. \d{2}[\dA-Z]{18}', // Saudi Arabia
3. 'SC' => 'SC\d{2}[A-Z]{4}\d{2}\d{2}\d{16}[A-Z]{3}', // Sey**chell**es
4. 'SD' => 'SD\d{2}\d{2}\d{12}', // Sudan

'SE' => 'SE\d{2}\d{3}\d{16}\d{1}', // Swed

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\var-dumper\Caster\ResourceCaster.php*(3.07K)(Date dernière modif. February 15 2024 13:23:52.)*65e0d9d8d3798f0175319ba0ec669d85**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **2155** du fichier; voici le contexte :
2. y\_get\_details($pin)['key'];
3. $pin = \array\_slice(explode("\n", $pin), 1, -2);
4. $pin = **base64\_decode**(implode('', $pin));
5. $pin = base64\_encode(hash('sha256', $pin, true));

$a += [

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\var-dumper\Server\DumpServer.php*(3.06K)(Date dernière modif. February 15 2024 13:23:52.)*52e46059d2718368392e8db2f26e8de4**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1543** du fichier; voici le contexte :
2. a payload from client {clientId}', ['clientId' => $clientId]);
3. $payload = @unserialize(**base64\_decode**($message), ['allowed\_classes' => [Data::class, Stub::class]]);

// Impossible to decode

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\symfony\yaml\Inline.php*(34.28K)(Date dernière modif. January 23 2024 16:51:36.)*fc997b90d795fb0e2898a7ca429bc84f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **34073** du fichier; voici le contexte :
2. inaryData), self::$parsedLineNumber + 1, $scalar, self::$parsedFilename);
3. }
4. return **base64\_decode**($parsedBinaryData, true);
5. }

private static function isBinaryString(string $value): bool

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\voku\portable-ascii\src\voku\helper\ASCII.php*(51.91K)(Date dernière modif. March 08 2022 19:03:00.)*6729043c09e00251d9331d49906a0c37**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **attacking**Trouvé en position **1520** du fichier; voici le contexte :
2. o people of Russia

\* There is a war in Ukraine right now. The forces of the Russian Federation are **attacking** civilian infrastructure in [Kharkiv][1], [Kyiv][2], [Chernihiv][3], [Sumy][4], [Irpin][5] and dozen

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\voku\portable-utf8\LICENSE-GPL*(17.20K)(Date dernière modif. March 08 2023 10:35:38.)*fcf5189e10b4f39d81f5320c35bc5bb8**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Hacker**Trouvé en position **17208** du fichier; voici le contexte :
2. copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James **Hacker**.
3. signature of Ty Coon, 1 April 1989
4. Ty Coon, President of Vice

This General Public License does n

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\voku\portable-utf8\src\voku\helper\data\emoji.php*(169.18K)(Date dernière modif. March 08 2023 10:35:38.)*5254be3545dee346a8192280972c5617**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **127210** du fichier; voici le contexte :

u{1F96E}", 'CHARACTER\_DANGO' => "\u{1F361}", 'CHARACTER\_DUMPLING' => "\u{1F95F}", 'CHARACTER\_FORTUNE**\_COOKIE**' => "\u{1F960}", 'CHARACTER\_TAKEOUT\_BOX' => "\u{1F961}", 'CHARACTER\_SOFT\_ICE\_CREAM' => "\u{1F366}",

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **127442** du fichier; voici le contexte :

> "\u{1F367}", 'CHARACTER\_ICE\_CREAM' => "\u{1F368}", 'CHARACTER\_DOUGHNUT' => "\u{1F369}", 'CHARACTER**\_COOKIE**' => "\u{1F36A}", 'CHARACTER\_BIRTHDAY\_CAKE' => "\u{1F382}", 'CHARACTER\_SHORTCAKE' => "\u{1F370}", 'C

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **SHELL**Trouvé en position **122976** du fichier; voici le contexte :

\u{1F421}", 'CHARACTER\_SHARK' => "\u{1F988}", 'CHARACTER\_OCTOPUS' => "\u{1F419}", 'CHARACTER\_SPIRAL\_**SHELL**' => "\u{1F41A}", 'CHARACTER\_CRAB' => "\u{1F980}", 'CHARACTER\_LOBSTER' => "\u{1F99E}", 'CHARACTER\_SH

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **CHELL**Trouvé en position **169567** du fichier; voici le contexte :

}\u{1F1E6}", 'CHARACTER\_FLAGS\_FOR\_SOLOMON\_ISLANDS' => "\u{1F1F8}\u{1F1E7}", 'CHARACTER\_FLAGS\_FOR\_SEY**CHELL**ES' => "\u{1F1F8}\u{1F1E8}", 'CHARACTER\_FLAGS\_FOR\_SUDAN' => "\u{1F1F8}\u{1F1E9}", 'CHARACTER\_FLAGS\_F

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\voku\portable-utf8\src\voku\helper\UTF8.php*(458.45K)(Date dernière modif. March 08 2023 10:35:38.)*a134a8f586f7348d7742206d8c87fcce**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **attacking**Trouvé en position **1520** du fichier; voici le contexte :
2. o people of Russia

\* There is a war in Ukraine right now. The forces of the Russian Federation are **attacking** civilian infrastructure in [Kharkiv][1], [Kyiv][2], [Chernihiv][3], [Sumy][4], [Irpin][5] and dozen

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **68438** du fichier; voici le contexte :

One of <b>INPUT\_GET</b>, <b>INPUT\_POST</b>,

\* <b>INPUT**\_COOKIE**</b>, <b>INPUT\_SERVER</b>, or

\* <b>INPUT\_ENV</b>.

\*

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **71028** du fichier; voici le contexte :

of <b>INPUT\_GET</b>, <b>INPUT\_POST</b>,

\* <b>INPUT**\_COOKIE**</b>, <b>INPUT\_SERVER</b>, or

\* <b>INPUT\_ENV</b>.

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **47933** du fichier; voici le contexte :

$from\_encoding = '';

}

if ($from\_encoding === 'BASE64') {

$str = \**base64\_decode**($str, true);

$from\_encoding = '';

}

if ($from\_encoding === 'HTML-ENTIT

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **129989** du fichier; voici le contexte :

}

if (!\is\_string($str)) {

return false;

}

$base64String = \**base64\_decode**($str, true);

return $base64String !== false && \base64\_encode($base64String) === $str;

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **336239** du fichier; voici le contexte :

rder version of UTF8::strcasecmp()

\*

\* EXAMPLES: <code>

\* UTF8::strnatcasecmp('2', '1**0Hell**o WORLD 中文空白!'); // -1

\* UTF8::strcasecmp('2Hello world 中文空白!', '1**0Hell**o WORLD

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **336300** du fichier; voici le contexte :

ode>

\* UTF8::strnatcasecmp('2', '10Hello WORLD 中文空白!'); // -1

\* UTF8::strcasecmp('**2Hell**o world 中文空白!', '10Hello WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcasecmp('10He

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **336331** du fichier; voici le contexte :

('2', '1**0Hell**o WORLD 中文空白!'); // -1

\* UTF8::strcasecmp('2Hello world 中文空白!', '1**0Hell**o WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcasecmp('1**0Hell**o world 中文空白!', '2Hel

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **336402** du fichier; voici le contexte :

ello world 中文空白!', '1**0Hell**o WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcasecmp('1**0Hell**o world 中文空白!', '2Hello WORLD 中文空白!'); // 1

\* UTF8::strcasecmp('1**0Hell**o world �

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **336432** du fichier; voici le contexte :

Hello WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcasecmp('10Hello world 中文空白!', '**2Hell**o WORLD 中文空白!'); // 1

\* UTF8::strcasecmp('10Hello world 中文空白!', '**2Hell**o WORLD �

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **336493** du fichier; voici le contexte :

asecmp('1**0Hell**o world 中文空白!', '2Hello WORLD 中文空白!'); // 1

\* UTF8::strcasecmp('1**0Hell**o world 中文空白!', '2Hello WORLD 中文空白!'); // -1

\* </code>

\*

\* @param str

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **336523** du fichier; voici le contexte :

�白!', '**2Hell**o WORLD 中文空白!'); // 1

\* UTF8::strcasecmp('10Hello world 中文空白!', '**2Hell**o WORLD 中文空白!'); // -1

\* </code>

\*

\* @param string $str1 <p>The first str

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **337542** du fichier; voici le contexte :

NFO: natural order version of UTF8::strcmp()

\*

\* EXAMPLES: <code>

\* UTF8::strnatcmp('**2Hell**o world 中文空白!', '10Hello WORLD 中文空白!'); // -1

\* UTF8::strcmp('**2Hell**o world 中�

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **337573** du fichier; voici le contexte :

TF8::strcmp()

\*

\* EXAMPLES: <code>

\* UTF8::strnatcmp('2Hello world 中文空白!', '1**0Hell**o WORLD 中文空白!'); // -1

\* UTF8::strcmp('2Hello world 中文空白!', '1**0Hell**o WORLD 中�

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **337630** du fichier; voici le contexte :

:strnatcmp('**2Hell**o world 中文空白!', '10Hello WORLD 中文空白!'); // -1

\* UTF8::strcmp('**2Hell**o world 中文空白!', '10Hello WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcmp('10Hello

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **337661** du fichier; voici le contexte :

空白!', '1**0Hell**o WORLD 中文空白!'); // -1

\* UTF8::strcmp('2Hello world 中文空白!', '1**0Hell**o WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcmp('1**0Hell**o world 中文空白!', '2Hello W

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **337728** du fichier; voici le contexte :

('2Hello world 中文空白!', '1**0Hell**o WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcmp('1**0Hell**o world 中文空白!', '2Hello WORLD 中文空白!'); // 1

\* UTF8::strcmp('1**0Hell**o world 中�

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **337758** du fichier; voici le contexte :

'10Hello WORLD 中文空白!'); // 1

\*

\* UTF8::strnatcmp('10Hello world 中文空白!', '**2Hell**o WORLD 中文空白!'); // 1

\* UTF8::strcmp('10Hello world 中文空白!', '**2Hell**o WORLD 中�

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **0Hell**Trouvé en position **337815** du fichier; voici le contexte :

:strnatcmp('1**0Hell**o world 中文空白!', '2Hello WORLD 中文空白!'); // 1

\* UTF8::strcmp('1**0Hell**o world 中文空白!', '2Hello WORLD 中文空白!'); // -1

\* </code>

\*

\* @see http:

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **2Hell**Trouvé en position **337845** du fichier; voici le contexte :

��空白!', '**2Hell**o WORLD 中文空白!'); // 1

\* UTF8::strcmp('10Hello world 中文空白!', '**2Hell**o WORLD 中文空白!'); // -1

\* </code>

\*

\* @see http://php.net/manual/en/function.s

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'Hell**Trouvé en position **387326** du fichier; voici le contexte :

haracters or replace sub-strings.

\*

\* EXAMPLE:

\* <code>

\* $array = [

\* **'Hell**o' => '○●◎',

\* '中文空白' => 'earth',

\* ];

\* UTF8::strtr(**'Hell**o 中�

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **'Hell**Trouvé en position **387419** du fichier; voici le contexte :

\* **'Hell**o' => '○●◎',

\* '中文空白' => 'earth',

\* ];

\* UTF8::strtr(**'Hell**o 中文空白', $array); // '○●◎ earth'

\* </code>

\*

\* @see http://php.net/manu

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\web-token\jwt-library\Console\SecretKeyGeneratorCommand.php*(2.00K)(Date dernière modif. February 28 2024 11:04:36.)*e800f84708b08bcdda650b04b999660f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1692** du fichier; voici le contexte :
2. nvalid option value for "is\_b64"');
3. }
4. if ($isBsae64Encoded) {
5. $secret = **base64\_decode**($secret, true);
6. }
7. if (! is\_string($secret)) {

throw new InvalidArgument

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\web-token\jwt-library\Encryption\Compression\Deflate.php*(1.75K)(Date dernière modif. February 28 2024 11:04:36.)*07ef44aa8f31ac2641d39e1aca1564d9**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **gzdeflate**Trouvé en position **879** du fichier; voici le contexte :
2. ';
3. }
4. public function compress(string $data): string
5. {
6. try {
7. $bin = **gzdeflate**($data, $this->getCompressionLevel());
8. if (! is\_string($bin)) {

throw ne

×

1. D:\wamp64\www\randophil.J5\libraries\vendor\web-token\jwt-library\KeyManagement\KeyConverter\KeyConverter.php*(12.51K)(Date dernière modif. February 28 2024 11:04:36.)*dca1da32f7e990b6a0978d2981f770ef**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **11799** du fichier; voici le contexte :
2. b));
3. $key = preg\_replace('#^(?:Proc-Type|DEK-Info): .\*#m', '', $pem);
4. $ciphertext = **base64\_decode**(preg\_replace('#-.\*-|\r|\n#', '', $key ?? '') ?? '', true);

if (! is\_string($ciphertext)) {

×

1. D:\wamp64\www\randophil.J5\media\vendor\bootstrap\css\bootstrap.css.map*(663.10K)(Date dernière modif. August 27 2024 02:32:22.)*8acd3942419907b180f8d5d0f0ffaff8**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **632323** du fichier; voici le contexte :

ing the scroll\n// .modal - container to scroll within\n// .modal-dialog - positioning **shell** for the actual modal\n// .modal-content - actual modal w/ bg and corners and stuff\n\n\n// Contai

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **634469** du fichier; voici le contexte :

t.org/show\_bug.cgi?id=158342\n // See also https://github.com/twbs/bootstrap/issues/17695\n}\n\n// **Shell** div to position the modal with bottom padding\n.modal-dialog {\n position: relative;\n width: aut

×

1. D:\wamp64\www\randophil.J5\media\vendor\bootstrap\css\bootstrap.min.css.map*(575.35K)(Date dernière modif. August 27 2024 02:32:22.)*ef5ca9e28f780a079318afab2334d8eb**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **542473** du fichier; voici le contexte :

ing the scroll\n// .modal - container to scroll within\n// .modal-dialog - positioning **shell** for the actual modal\n// .modal-content - actual modal w/ bg and corners and stuff\n\n\n// Contai

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **544619** du fichier; voici le contexte :

t.org/show\_bug.cgi?id=158342\n // See also https://github.com/twbs/bootstrap/issues/17695\n}\n\n// **Shell** div to position the modal with bottom padding\n.modal-dialog {\n position: relative;\n width: aut

×

1. D:\wamp64\www\randophil.J5\media\vendor\bootstrap\scss\\_modal.scss*(7.58K)(Date dernière modif. August 27 2024 02:32:22.)*1dc2a53cddb54f8647ba38eb1b7e49b1**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **shell**Trouvé en position **186** du fichier; voici le contexte :
2. lling the scroll
3. // .modal - container to scroll within
4. // .modal-dialog - positioning **shell** for the actual modal
5. // .modal-content - actual modal w/ bg and corners and stuff

// Container

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **Shell**Trouvé en position **2285** du fichier; voici le contexte :

ebkit.org/show\_bug.cgi?id=158342

// See also https://github.com/twbs/bootstrap/issues/17695

}

// **Shell** div to position the modal with bottom padding

.modal-dialog {

position: relative;

width: auto;

×

1. D:\wamp64\www\randophil.J5\media\vendor\fontawesome-free\scss\\_shims.scss*(67.46K)(Date dernière modif. August 27 2024 02:32:22.)*a269ab810a51cbf72a026eb4651e96ac**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **40882** du fichier; voici le contexte :
2. font-family: 'Font Awesome 6 Brands';
3. font-weight: 400;
4. }
5. .#{$fa-css-prefix}.#{$fa-css-prefix}-**hacker**-news {
6. font-family: 'Font Awesome 6 Brands';
7. font-weight: 400;
8. }

.#{$fa-css-prefix}.#{$fa-css-

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **41177** du fichier; voici le contexte :

}

.#{$fa-css-prefix}.#{$fa-css-prefix}-y-combinator-square:before { content: unquote("\"#{ $fa-var-**hacker**-news }\""); }

.#{$fa-css-prefix}.#{$fa-css-prefix}-yc-square {

font-family: 'Font Awesome 6 Bran

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **41397** du fichier; voici le contexte :

ight: 400;

}

.#{$fa-css-prefix}.#{$fa-css-prefix}-yc-square:before { content: unquote("\"#{ $fa-var-**hacker**-news }\""); }

.#{$fa-css-prefix}.#{$fa-css-prefix}-tencent-weibo {

font-family: 'Font Awesome 6

×

1. D:\wamp64\www\randophil.J5\media\vendor\fontawesome-free\scss\\_variables.scss*(158.82K)(Date dernière modif. August 27 2024 02:32:22.)*f96d556b9e16a0282da59fcb3e9bd7e0**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **57804** du fichier; voici le contexte :
2. var-instagram-square: \e055;
3. $fa-var-battle-net: \f835;
4. $fa-var-the-red-yeti: \f69d;
5. $fa-var-square-**hacker**-news: \f3af;
6. $fa-var-**hacker**-news-square: \f3af;
7. $fa-var-edge: \f282;
8. $fa-var-threads: \e618;

$fa-va

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **57832** du fichier; voici le contexte :

$fa-var-battle-net: \f835;

$fa-var-the-red-yeti: \f69d;

$fa-var-square-**hacker**-news: \f3af;

$fa-var-**hacker**-news-square: \f3af;

$fa-var-edge: \f282;

$fa-var-threads: \e618;

$fa-var-napster: \f3d2;

$fa-var-sq

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **58673** du fichier; voici le contexte :

al-ocean: \f391;

$fa-var-nimblr: \f5a8;

$fa-var-chromecast: \f838;

$fa-var-evernote: \f839;

$fa-var-**hacker**-news: \f1d4;

$fa-var-creative-commons-sampling: \f4f0;

$fa-var-adversal: \f36a;

$fa-var-creative-co

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **61689** du fichier; voici le contexte :

amework: \f3dc;

$fa-var-shopify: \e057;

$fa-var-neos: \f612;

$fa-var-square-threads: \e619;

$fa-var-**hacker**rank: \f5f7;

$fa-var-researchgate: \f4f8;

$fa-var-swift: \f8e1;

$fa-var-angular: \f420;

$fa-var-spea

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **146582** du fichier; voici le contexte :

agram-square,

"battle-net": $fa-var-battle-net,

"the-red-yeti": $fa-var-the-red-yeti,

"square-**hacker**-news": $fa-var-square-**hacker**-news,

"**hacker**-news-square": $fa-var-**hacker**-news-square,

"edge": $f

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **146611** du fichier; voici le contexte :

$fa-var-battle-net,

"the-red-yeti": $fa-var-the-red-yeti,

"square-**hacker**-news": $fa-var-square-**hacker**-news,

"**hacker**-news-square": $fa-var-**hacker**-news-square,

"edge": $fa-var-edge,

"threads": $fa-

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **146627** du fichier; voici le contexte :

net,

"the-red-yeti": $fa-var-the-red-yeti,

"square-**hacker**-news": $fa-var-square-**hacker**-news,

"**hacker**-news-square": $fa-var-**hacker**-news-square,

"edge": $fa-var-edge,

"threads": $fa-var-threads,

"

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **146656** du fichier; voici le contexte :

r-the-red-yeti,

"square-**hacker**-news": $fa-var-square-**hacker**-news,

"**hacker**-news-square": $fa-var-**hacker**-news-square,

"edge": $fa-var-edge,

"threads": $fa-var-threads,

"napster": $fa-var-napster,

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **147769** du fichier; voici le contexte :

"nimblr": $fa-var-nimblr,

"chromecast": $fa-var-chromecast,

"evernote": $fa-var-evernote,

"**hacker**-news": $fa-var-**hacker**-news,

"creative-commons-sampling": $fa-var-creative-commons-sampling,

"ad

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **147791** du fichier; voici le contexte :

imblr,

"chromecast": $fa-var-chromecast,

"evernote": $fa-var-evernote,

"**hacker**-news": $fa-var-**hacker**-news,

"creative-commons-sampling": $fa-var-creative-commons-sampling,

"adversal": $fa-var-adver

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **151749** du fichier; voici le contexte :

"shopify": $fa-var-shopify,

"neos": $fa-var-neos,

"square-threads": $fa-var-square-threads,

"**hacker**rank": $fa-var-**hacker**rank,

"researchgate": $fa-var-researchgate,

"swift": $fa-var-swift,

"angu

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **151770** du fichier; voici le contexte :

hopify,

"neos": $fa-var-neos,

"square-threads": $fa-var-square-threads,

"**hacker**rank": $fa-var-**hacker**rank,

"researchgate": $fa-var-researchgate,

"swift": $fa-var-swift,

"angular": $fa-var-angular

×

1. D:\wamp64\www\randophil.J5\modules\mod\_jm\_kick\_cass\tmpl\default.php*(23.73K)(Date dernière modif. March 26 2022 15:53:54.)*b390f510efd2f44038bf0c5380a6afab**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **510** du fichier; voici le contexte :
2. tInstance();
3. $base=$uri->base();
4. $cc\_textdecoration = $params->get('textdedoration', '0');
5. $cc**\_cookie**notice = $params->get('CookieNotice');
6. $cc\_popup = $params->get('Popup');

$cc\_s

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **6726** du fichier; voici le contexte :

ho $params->get('ShareNumber')?>

}

});

};

</script>

<?php

}

if ($cc**\_cookie**notice){

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*//

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

×

1. D:\wamp64\www\randophil.J5\plugins\api-authentication\token\src\Extension\Token.php*(13.03K)(Date dernière modif. August 27 2024 02:31:12.)*087ea607ea050831df341e8c23ef6835**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4741** du fichier; voici le contexte :
2. // The token is a base64 encoded string. Make sure we can decode it.
3. $authString = @**base64\_decode**($tokenString);

if (empty($authString) || (strpos($authString, ':') === false)) {

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **6021** du fichier; voici le contexte :

nceTokenData = empty($referenceTokenData) ? '' : $referenceTokenData;

$referenceTokenData = **base64\_decode**($referenceTokenData);

$referenceHMAC = hash\_hmac($algo, $referenceTokenData, $siteSecr

×

1. D:\wamp64\www\randophil.J5\plugins\authentication\cookie\src\Extension\Cookie.php*(14.12K)(Date dernière modif. August 27 2024 02:31:12.)*0879343fd00bf5b54026e37e22a43470**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **813** du fichier; voici le contexte :
2. cation plugin
3. \*
4. \* @since 3.2
5. \* @note Code based on http://jaspan.com/improved\_persistent\_login**\_cookie**\_best\_practice

\* and http://fishbowl.pastiche.org/2004/01/19/persistent\_login**\_cookie**\_best\_p

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **906** du fichier; voici le contexte :

t\_login**\_cookie**\_best\_practice

\* and http://fishbowl.pastiche.org/2004/01/19/persistent\_login**\_cookie**\_best\_practice/

\*/

final class Cookie extends CMSPlugin

{

use DatabaseAwareTrait;

use UserF

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1378** du fichier; voici le contexte :

guage();

return [

$this->getApplication()->getLanguage()->\_('PLG\_AUTHENTICATION**\_COOKIE**') => [

$this->getApplication()->getLanguage()->\_('PLG\_AUTHENTICATION**\_COOKIE**\_PRIVACY

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1470** du fichier; voici le contexte :

TICATION**\_COOKIE**') => [

$this->getApplication()->getLanguage()->\_('PLG\_AUTHENTICATION**\_COOKIE**\_PRIVACY\_CAPABILITY**\_COOKIE**'),

],

];

}

/\*\*

\* This method should han

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **1496** du fichier; voici le contexte :

$this->getApplication()->getLanguage()->\_('PLG\_AUTHENTICATION**\_COOKIE**\_PRIVACY\_CAPABILITY**\_COOKIE**'),

],

];

}

/\*\*

\* This method should handle any authentication and

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **6112** du fichier; voici le contexte :

Issue warning by email to user and/or admin?

Log::add(Text::sprintf('PLG\_AUTHENTICATION**\_COOKIE**\_ERROR\_LOG\_LOGIN\_FAILED', $results[0]->user\_id), Log::WARNING, 'security');

$response->s

×

1. D:\wamp64\www\randophil.J5\plugins\installer\webinstaller\src\Extension\WebInstaller.php*(5.50K)(Date dernière modif. August 27 2024 02:31:12.)*b2fc92b32b2a06766683ce0563eb5b5d**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4986** du fichier; voici le contexte :
2. nction getInstallFrom()
3. {
4. if ($this->installfrom === null) {
5. $installfrom = **base64\_decode**($this->getApplication()->getInput()->getBase64('installfrom', ''));

$field = new \Simp

×

1. D:\wamp64\www\randophil.J5\plugins\multifactorauth\webauthn\src\Extension\Webauthn.php*(16.77K)(Date dernière modif. August 27 2024 02:31:12.)*d3a55e98382ca0bd5b9cd955c7360fb7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **13238** du fichier; voici le contexte :
2. ion (good): we do not have a pending key request');
3. }
4. $serializedOptions = **base64\_decode**($pkOptionsEncoded);

$pkOptions = unserialize($serializedOptions);

×

1. D:\wamp64\www\randophil.J5\plugins\multifactorauth\webauthn\src\Helper\Credentials.php*(12.73K)(Date dernière modif. August 27 2024 02:31:12.)*a80c13c7ca2c414ee756015943c825b6**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **4221** du fichier; voici le contexte :
2. TE\_NO\_PK'));
3. }
4. try {
5. $publicKeyCredentialCreationOptions = unserialize(**base64\_decode**($encodedOptions));
6. } catch (\Exception $e) {

$publicKeyCredentialCreationOption

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **5272** du fichier; voici le contexte :

return self::getWebauthnServer($myUser->id)->loadAndCheckAttestationResponse(

**base64\_decode**($data),

$publicKeyCredentialCreationOptions,

ServerRequestFactory::fromGlob

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **8812** du fichier; voici le contexte :

ey credential request options in the session are valid

$serializedOptions = **base64\_decode**($encodedPkOptions);

$publicKeyCredentialRequestOptions = unserialize($serializedOptions);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9356** du fichier; voici le contexte :

VALID\_LOGIN\_REQUEST'));

}

// Unserialize the browser response data

$data = **base64\_decode**($response);

self::getWebauthnServer($user->id)->loadAndCheckAssertionResponse(

×

1. D:\wamp64\www\randophil.J5\plugins\multifactorauth\yubikey\src\Extension\Yubikey.php*(20.62K)(Date dernière modif. August 27 2024 02:31:12.)*cd5a0c822384caccd0ab928adbd5ff7f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17161** du fichier; voici le contexte :
2. d base64 encoding and decoding
3. if (!\function\_exists('base64\_encode') || !\function\_exists('**base64\_decode**')) {
4. return;
5. }

// I need HMAC-SHA-1 support. Therefore I check for HMA

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **19085** du fichier; voici le contexte :

ber to

\* base64decode the API key obtained from Yubico).

\*/

$decodedKey = **base64\_decode**($secret);

$hash = hash\_hmac('sha1', $stringToSign, $decodedKey, true);

/\*\*

×

1. D:\wamp64\www\randophil.J5\plugins\sampledata\multilang\src\Extension\MultiLanguage.php*(43.09K)(Date dernière modif. August 27 2024 02:31:12.)*722b7bcd537046d05f84333d24eed6ca**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **16031** du fichier; voici le contexte :
2. '"item\_associations":"1",'
3. . '"remove\_default\_prefix":"0",'
4. . '"lang**\_cookie**":"0",'
5. . '"alternate\_meta":"1"'
6. . '}';

$query

×

1. D:\wamp64\www\randophil.J5\plugins\system\debug\src\DataCollector\RequestDataCollector.php*(1.87K)(Date dernière modif. August 27 2024 02:31:12.)*31d186696fe3baa1cc79c06a5e0419b8**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **861** du fichier; voici le contexte :
2. ay
3. \*/
4. public function collect()
5. {
6. $vars = ['\_GET', '\_POST', '\_SESSION', '**\_COOKIE**', '\_SERVER'];
7. $returnData = [];
8. foreach ($vars as $var) {

if (isset($G

×

1. D:\wamp64\www\randophil.J5\plugins\system\highlight\src\Extension\Highlight.php*(3.61K)(Date dernière modif. August 27 2024 02:31:12.)*6b1a2e6fe1c0ddf981a84b276ef856c7**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1899** du fichier; voici le contexte :
2. $terms = $input->request->get('highlight', null, 'base64');
3. $terms = $terms ? json\_decode(**base64\_decode**($terms)) : null;
4. // Check the terms.
5. if (empty($terms)) {

return;

×

1. D:\wamp64\www\randophil.J5\plugins\system\jsvisit\_counter\countries.csv*(4.87K)(Date dernière modif. July 15 2024 18:05:06.)*dafe3dbc82284db037bf13be273f009a**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **chell**Trouvé en position **3829** du fichier; voici le contexte :
2. Marino,SM,674
3. Sao Tome and Principe,ST,678
4. Saudi Arabia,SA,682
5. Senegal,SN,686
6. Serbia,RS,688
7. Sey**chell**es,SC,690
8. Sierra Leone,SL,694
9. Singapore,SG,702
10. Sint Maarten (Dutch part),SX,534

Slovakia,SK,703

×

1. D:\wamp64\www\randophil.J5\plugins\system\jsvisit\_counter\helper.php*(41.72K)(Date dernière modif. July 15 2024 18:05:06.)*91f496ab02587be313cac66f24236e65**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **ia\_archiver**Trouvé en position **16372** du fichier; voici le contexte :
2. $bots = array(
3. 'Googlebot',
4. 'Baiduspider',
5. '**ia\_archiver**',
6. 'R6\_FeedFetcher',
7. 'NetcraftSurveyAgent',

'Sogo

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **BackDoor**Trouvé en position **24570** du fichier; voici le contexte :

'BBBike',

'BDCbot',

'BDFetch',

'**BackDoor**Bot',

'BackStreet',

'BackWeb',

'Backlink-Ceck',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **HackTeam**Trouvé en position **36320** du fichier; voici le contexte :

'Suzuran',

'Swiftbot',

'Szukacz',

'T0P**HackTeam**',

'T8Abot',

'Teleport',

'TeleportPro',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **38397** du fichier; voici le contexte :

'WebSauger',

'WebStripper',

'WebSucker',

'WebW**hacker**',

'WebZIP',

'Web Auto',

'Web Collage',

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **38956** du fichier; voici le contexte :

'Website Quester',

'Webster',

'Whack',

'W**hacker**',

'Whatweb',

'Who.is Bot',

'Widow',

×

1. D:\wamp64\www\randophil.J5\plugins\system\languagefilter\src\Extension\LanguageFilter.php*(33.02K)(Date dernière modif. August 27 2024 02:31:12.)*d58d030a637e66487578f26a7adac028**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **18085** du fichier; voici le contexte :
2. $this->getApplication()->getLanguage()->\_('PLG\_SYSTEM\_LANGUAGEFILTER\_PRIVACY\_CAPABILITY\_LANGUAGE**\_COOKIE**'),
3. ],
4. ];
5. }
6. /\*\*
7. \* Before store user method.
8. \*

\* Method i

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **32091** du fichier; voici le contexte :

in plugin params, save the user language in a new cookie.

if ((int) $this->params->get('lang**\_cookie**', 0) === 1) {

// Create a cookie with one year lifetime.

$this->getApplicat

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **33252** du fichier; voici le contexte :

in plugin params, get the user language from the cookie.

if ((int) $this->params->get('lang**\_cookie**', 0) === 1) {

$languageCode = $this->getApplication()->getInput()->cookie->get(Applicat

×

1. D:\wamp64\www\randophil.J5\plugins\system\redirect\src\Extension\Redirect.php*(9.10K)(Date dernière modif. August 27 2024 02:31:12.)*48b2faf5d4b9e6ea8049336330791383**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **3996** du fichier; voici le contexte :
2. }
3. }
4. }
5. /\*\*
6. \* Why is this (still) here?

\* Because **hacker**s still try urls with mosConfig\_\* and Url Injection with =http[s]:// and we dont want to log/redirec

×

1. **Attention** D:\wamp64\www\randophil.J5\plugins\system\webauthn\fido.jwt*Ce fichier a été ignoré car sa taille excède la taille max. autorisée (4M)*

×

1. D:\wamp64\www\randophil.J5\plugins\system\webauthn\src\Authentication.php*(19.10K)(Date dernière modif. August 27 2024 02:31:12.)*7739412d4e69803c75133941afaac43a**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9024** du fichier; voici le contexte :
2. em\_webauthn.publicKeyCredentialRequestOptions', null);
3. $serializedOptions = **base64\_decode**($encodedPkOptions);

$publicKeyCredentialRequestOptions = unserialize($serializedOptions);

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **9660** du fichier; voici le contexte :

eption(Text::\_('PLG\_SYSTEM\_WEBAUTHN\_ERR\_CREATE\_INVALID\_LOGIN\_REQUEST'));

}

$data = **base64\_decode**($data);

if (empty($data)) {

Log::add('No or invalid assertion data received fr

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **11620** du fichier; voici le contexte :

ntialCreationOptions \*/

try {

$publicKeyCredentialCreationOptions = unserialize(**base64\_decode**($encodedOptions));

} catch (\Exception $e) {

Log::add('The plg\_system\_webauthn.

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **12966** du fichier; voici le contexte :

g Diactoros

return $this->getWebauthnServer()->loadAndCheckAttestationResponse(

**base64\_decode**($data),

$publicKeyCredentialCreationOptions,

ServerRequestFactory::fromGlob

**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17990** du fichier; voici le contexte :

N\_REQUEST'));

}

try {

$publicKeyCredentialRequestOptions = unserialize(**base64\_decode**($encodedOptions));

} catch (\Exception $e) {

Log::add('Invalid plg\_system\_webau

×

1. D:\wamp64\www\randophil.J5\plugins\system\webauthn\src\PluginTraits\AjaxHandlerChallenge.php*(3.17K)(Date dernière modif. August 27 2024 02:31:12.)*efaac564da17c7fc380adeb539fee430**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1803** du fichier; voici le contexte :
2. ))
3. );
4. $returnUrl = $input->getBase64('returnUrl', $returnUrl);
5. $returnUrl = **base64\_decode**($returnUrl);

// For security reasons the post-login redirection URL must be internal to th

×

1. D:\wamp64\www\randophil.J5\plugins\system\webauthn\src\PluginTraits\AjaxHandlerCreate.php*(4.72K)(Date dernière modif. August 27 2024 02:31:12.)*9deaf97706de08c13108c2affeeb257b**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **hacker**Trouvé en position **2560** du fichier; voici le contexte :
2. tem\_webauthn.publicKeyCredentialCreationOptions', null);
3. // Politely tell the presumed **hacker** trying to abuse this callback to go away.

throw new \RuntimeException(Text::\_('PLG\_SYST

×

1. D:\wamp64\www\randophil.J5\plugins\system\webauthn\src\PluginTraits\AjaxHandlerDelete.php*(2.25K)(Date dernière modif. August 27 2024 02:31:12.)*865d6c85fc0ad85fdc925194717dced9**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1376** du fichier; voici le contexte :
2. d)) {
3. $event->addResult(false);
4. return;
5. }
6. $credentialId = **base64\_decode**($credentialId);

if (empty($credentialId) || !$repository->has($credentialId)) {

×

1. D:\wamp64\www\randophil.J5\plugins\system\webauthn\src\PluginTraits\AjaxHandlerSaveLabel.php*(2.51K)(Date dernière modif. August 27 2024 02:31:12.)*25db6d70ce86187234b2e06ede4c57fd**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **1477** du fichier; voici le contexte :
2. d)) {
3. $event->addResult(false);
4. return;
5. }
6. $credentialId = **base64\_decode**($credentialId);

if (empty($credentialId) || !$repository->has($credentialId)) {

×

1. D:\wamp64\www\randophil.J5\plugins\user\token\src\Extension\Token.php*(19.01K)(Date dernière modif. August 27 2024 02:31:12.)*e8d13942518431fa97792778b660768f**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **17524** du fichier; voici le contexte :
2. u monster!
3. if (empty($siteSecret)) {
4. return '';
5. }
6. $rawToken = **base64\_decode**($tokenSeed);
7. $tokenHash = hash\_hmac($algorithm, $rawToken, $siteSecret);

$message

×

1. D:\wamp64\www\randophil.J5\plugins\user\token\src\Field\JoomlatokenField.php*(4.09K)(Date dernière modif. August 27 2024 02:31:12.)*b6cc60ee0a9e85a9fb512c93a9ae0473**Attention** Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.Signature : **base64\_decode**Trouvé en position **3539** du fichier; voici le contexte :
2. u monster!
3. if (empty($siteSecret)) {
4. return '';
5. }
6. $rawToken = **base64\_decode**($tokenSeed);
7. $tokenHash = hash\_hmac($algorithm, $rawToken, $siteSecret);

$userId