(https://github.com/AFUJ/quickscan/) 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. 1.537 fichiers | 3. Scanner le site | 4. Supprimer ce script du serveur

1.537 fichiers vont être analysés (11.957 fichiers ont été ignorés car ils sont repris sur la liste blanche d'aeSecure et 2.410 ignorés comme paramétré dans l'écran des options avancées).

1 -> 500 | 501 -> 1.000 | 1.001 -> 1.500 | 1.501 -> 1.537

1537 fichiers ont été analysés dont 34 sont détectés comme potentiellement dangereux.
0 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. /home/vx3xycwr/economie.pennes-mirabeau.org/components/com_convertforms/views/form/view.html.php

(1.57K) (Date dernière modif. March 04 2026 15:50:57.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 37656f79fdabb51cb277a0ea4c2e4d90 utilisé est néanmoins suspect.
Signature : **Hell**
Trouvé en position **526** du fichier; voici le contexte :

```
ories view.
 *
 * @since  1.5
 */
class ConvertFormsViewForm extends HtmlView
{
        /**
         * Display the Hello World view
         *
         * @param   string  $tpl  The name of the template file to parse; automatically
```

2. /home/vx3xycwr/economie.pennes-mirabeau.org/components/com_convertforms/views/submission/view.htm

(2.33K) (Date dernière modif. March 04 2026 15:50:57.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 1c6dd10fba898a9d15788835ac0015b4 utilisé est néanmoins suspect.
Signature : **Hell**
Trouvé en position **591** du fichier; voici le contexte :

```
view.
 *
 * @since  1.5
 */
class ConvertFormsViewSubmission extends HtmlView
{
        /**
         * Display the Hello World view
         *
         * @param   string  $tpl  The name of the template file to parse; automatically
```

3. /home/vx3xycwr/economie.pennes-mirabeau.org/libraries/astroid/framework/library/vendor/league/uri/Uri.php

(63.18K) (Date dernière modif. March 04 2026 14:53:45.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef ddf34d4e323e3c053364bbf4f94b97c1 utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **1275** du fichier; voici le contexte :

```
ay_key_last;
use function array_map;
use function array_pop;
use function array_shift;
use function base64_decode;
use function base64_encode;
use function basename;
use function count;
use function dirname;
use f
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **21478** du fichier; voici le contexte :

```
if (str_starts_with(strtolower($server['HTTP_AUTHORIZATION']), 'basic')) {
            $userinfo = base64_decode(substr($server['HTTP_AUTHORIZATION'], 6), true);
            false !== $userinfo || throw new Synta
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **27211** du fichier; voici le contexte :

```
arameters.'` is invalid.');
        if (!$isBinary) {
            return;
        }

        $res = base64_decode($data, true);
        if (false === $res || $data !== base64_encode($res)) {
            throw new
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **41900** du fichier; voici le contexte :

```
$data = match (true) {
            str_ends_with((string) $mediaType, ';base64') => (string) base64_decode($do
            default => rawurldecode($document),
        };

        $res = match
```

4. /home/vx3xycwr/economie.pennes-mirabeau.org/libraries/astroid/framework/library/vendor/phenx/php-font-lib

(1.90K) (Date dernière modif. March 04 2026 14:57:23.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé f04e7aacf64f4e41f526748a0e9f7c21 est néanmoins suspect.
Signature : **gzuncompress**
Trouvé en position **1047** du fichier; voici le contexte :

```
s->read($entry->length);

      if ($entry->length < $entry->origLength) {
        $data = (string) gzuncompress($data);
      }

      // Prepare data ...
      $length        = mb_strlen($data, '8bit');
      $
```

5. /home/vx3xycwr/economie.pennes-mirabeau.org/libraries/astroid/framework/library/astroid/Framework.php

(4.25K) (Date dernière modif. March 04 2026 14:48:44.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 8b2da4a8dbbf4f380f3bed21f41a9eda utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **3697** du fichier; voici le contexte :

```
ut->get->get('ast', '', 'RAW');
            if (!empty($redirect)) {
                $app->redirect(base64_decode(urldecode($redirect)));
            }
        }
    }

    public static function getClientType()
```

6. /home/vx3xycwr/economie.pennes-mirabeau.org/administrator/components/com_convertforms/ConvertForm

(2.26K) (Date dernière modif. March 04 2026 15:50:57.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 274362287ef900b7bea952bd054951e6 utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1314** du fichier; voici le contexte :

```
nsrr') && function_exists('exec') && is_callable('exec'))
                {
                        @exec('nslookup -type=MX ' . escapeshellcmd($domain), $output);

                        foreach($output as $line)
                        {
                                if (preg_match('/^' . preg_quote($dom
```

7. /home/vx3xycwr/economie.pennes-mirabeau.org/administrator/components/com_convertforms/ConvertForm

(3.38K) (Date dernière modif. March 04 2026 15:50:57.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 0787229ca6937119384bb8b0dc5eb2bf utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **1652** du fichier; voici le contexte :

```
$field_name = $this->field->get('name');

                // Decoded the signature
                $decoded_image_data = base64_decode(preg_replace('#^data:image/\w+;base

                // Path of the temporary signature
```

8. /home/vx3xycwr/economie.pennes-mirabeau.org/administrator/components/com_convertforms/ConvertForm

(14.10K) (Date dernière modif. March 04 2026 15:50:57.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 4fe8e63d5f450bc3c26d2d2a04a1e450 utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **2833** du fichier; voici le contexte :

```
}

                // Validate file paths
                foreach ($value as $key => &$source_file)
                {
                        $source_file = base64_decode($source_file);
                        $source_file_info = File::pathinfo($source_file);
                        $source_basename = $source
```

9. /home/vx3xycwr/economie.pennes-mirabeau.org/administrator/components/com_convertforms/ConvertForm

(5.06K) (Date dernière modif. March 04 2026 15:50:57.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef bd071344935dc62d671ca661c70f8ce1 utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **2459** du fichier; voici le contexte :

```
return $encrypted;
        }

        // Decode the base64 encoded string
        $data = base64_decode($encrypted, true);

        if ($data === false)
        {
            return null;
        }
```

10. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertforms/aweber/wrapper/aweber_api.php

(8.64K) (Date dernière modif. March 04 2026 15:50:58.)

Danger Ce mot est un mot ayant été encodé en base64 et 47ef3388c9f94c328b225414b27183a4 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 **8465** du fichier; voici le contexte :

```
tokens
         * on the user before calling this function via:
         *
         *    $aweber->user->tokenSecret  = $_COOKIE['requestTokenSecret'];
         *    $aweber->user->requestToken = $_GET['oauth_token'];
         *    $aweber->u
```

11. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/exportsubmissions/exportsubmis

(4.98K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef fb8e565ebc67f1ceb0bb0aee01b286ed utilisé est néanmoins suspect.
Signature : **'Hell**
Trouvé en position **4041** du fichier; voici le contexte :

```
s - Form Submissions Report - %s', $formName),
                    'body'        => Text::sprintf('Hello,<br><br>Please find attached
```

12. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/dompdf/dompdf/src/I

(37.64K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 307e20c2dd47526dafa9452f45b5f90f utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **9957** du fichier; voici le contexte :

```
'mime' => $match['mime'] ? $match['mime'] : 'text/plain',
            'data' => $match['base64'] ? base64_decode($match['data']) : $match['data']
        ];

        return $result;
    }

    /**
     * Encodes
```

13. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/dompdf/dompdf/src/(

(10.45K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 0faec2a5f1d041c037ea61a20681b024 utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **4448** du fichier; voici le contexte :

```
"salmon" => "FA8072",
        "sandybrown" => "F4A460",
        "seagreen" => "2E8B57",
        "seashell" => "FFF5EE",
        "sienna" => "A0522D",
        "silver" => "C0C0C0",
        "skyblue" => "87C
```

14. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/dompdf/dompdf/lib/C

(215.93K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef ad2f29faca1b872773e80f144d02da3b utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **11404** du fichier; voici le contexte :

```
_dir());
        $this->newDocument($pageSize);

        $this->compressionReady = function_exists('gzcompress');

        if (in_array('Windows-1252', mb_list_encodings())) {
            self::$targetEncoding
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **42191** du fichier; voici le contexte :

```
dths'][$cid] = $width;
                    }

                    $font['CIDtoGID'] = base64_encode(gzcompress($cidtogid));
                    $font['CIDtoGID_Compressed'] = true;

                    $data =
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **55931** du fichier; voici le contexte :

```
Name = $o['info']['fontFileName'];
                $tmp = $this->fonts[$fontFileName]['CIDtoGID'] = base64_decode($this->f

                $compressed = isset($this->fonts[$fontFi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **56565** du fichier; voici le contexte :

```
n on this content stream
                        $compressed = true;
                        $tmp = gzcompress($tmp, 6);
                    }
                    if ($compressed) {
                        $res
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **70461** du fichier; voici le contexte :

```
tent stream
                        $res .= " /Filter /FlateDecode";
                        $tmp = gzcompress($tmp, 6);
                    }

                    if ($this->encrypted) {
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **83723** du fichier; voici le contexte :

```
is content stream
                    $res .= " /Filter /FlateDecode\n";
                    $tmp = gzcompress($tmp, 6);
                }

                if ($this->encrypted) {
                    $this->enc
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **91836** du fichier; voici le contexte :

```
));
                list($head, $signature) = explode("\n\n", $sign);

                $signature = base64_decode(trim($signature));

                $signature = current(unpack('H*', $signature));
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **121138** du fichier; voici le contexte :

```
on CIDtoGID string
                $data['CIDtoGID_Compressed'] = true;
                $cidtogid = gzcompress($cidtogid, 6);
            }
            $data['CIDtoGID'] = base64_encode($cidtogid);
```

15. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/phenx/php-font-lib/sr

(1.95K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 66d51b973c667deb9a689c093bbd5183 utilisé est néanmoins suspect.
Signature : **gzuncompress**
Trouvé en position **1101** du fichier; voici le contexte :

```
s->read($entry->length);

      if ($entry->length < $entry->origLength) {
        $data = (string) gzuncompress($data);
      }

      // Prepare data ...
      $length        = mb_strlen($data, '8bit');
      $
```

16. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/phenx/php-svg-lib/sr

(17.91K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef eb1ab7d16a75722272d9d8c35e28ca4a utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **17940** du fichier; voici le contexte :

```
'saddlebrown'          => '#8b4513',
        'sandybrown'           => '#f4a460',
        'seashell'             => '#fff5ee',
        'slateblue'            => '#6a5acd',
        'slategrey'
```

17. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/phenx/php-svg-lib/sr

(11.49K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 7307a37a5c392b529c69871d315619ed utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **4059** du fichier; voici le contexte :

```
strpos($image, ";") + 1);
            if (strpos($data, "base64") === 0) {
                $data = base64_decode(substr($data, 7));
            }
        }
        else {
            $data = file_get_contents($im
```

18. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/phenx/php-svg-lib/sr

(13.43K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 5d275c63469c156d596d915ac2e1402f utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **4089** du fichier; voici le contexte :

```
$token = strtok(';');
            }

            if ($base64) {
                $data = base64_decode($data);
            }
        }
        else {
            $data = file_get_contents($image);
```

19. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/convertformstools/pdf/dompdf/phenx/php-svg-lib/sr

(212.65K) (Date dernière modif. March 04 2026 15:51:01.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef edc16e6108b43790e9bfdf628f055a29 utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **11708** du fichier; voici le contexte :

```
_dir());
        $this->newDocument($pageSize);

        $this->compressionReady = function_exists('gzcompress');

        if (in_array('Windows-1252', mb_list_encodings())) {
            self::$targetEncoding
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **53653** du fichier; voici le contexte :

```
Name = $o['info']['fontFileName'];
                $tmp = $this->fonts[$fontFileName]['CIDtoGID'] = base64_decode($this->f

                $compressed = isset($this->fonts[$fontFi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **54287** du fichier; voici le contexte :

```
n on this content stream
                        $compressed = true;
                        $tmp = gzcompress($tmp, 6);
                    }
                    if ($compressed) {
                        $res
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **68160** du fichier; voici le contexte :

```
tent stream
                        $res .= " /Filter /FlateDecode";
                        $tmp = gzcompress($tmp, 6);
                    }

                    if ($this->encrypted) {
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **81441** du fichier; voici le contexte :

```
is content stream
                    $res .= " /Filter /FlateDecode\n";
                    $tmp = gzcompress($tmp, 6);
                }

                if ($this->encrypted) {
                    $this->enc
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **89554** du fichier; voici le contexte :

```
));
                list($head, $signature) = explode("\n\n", $sign);

                $signature = base64_decode(trim($signature));

                $signature = current(unpack('H*', $signature));
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **119370** du fichier; voici le contexte :

```
on CIDtoGID string
                $data['CIDtoGID_Compressed'] = true;
                $cidtogid = gzcompress($cidtogid, 6);
            }
            $data['CIDtoGID'] = base64_encode($cidtogid);
```

20. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/tgeoip/vendor/splitbrain/php-archive/src/Zip

(32.78K) (Date dernière modif. March 04 2026 15:51:02.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 60202250baf16c2ad286630d7d712ed1 utilisé est néanmoins suspect.
Signature : **gzcompress**
Trouvé en position **13672** du fichier; voici le contexte :

```
\strlen($data);
        $crc = \crc32($data);
        if ($this->complevel) {
            $data = \gzcompress($data, $this->complevel);
            $data = \substr($data, 2, -4);
            // strip compressi
```

21. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/tgeoip/vendor/composer/ca-bundle/src/CaB

(16.99K) (Date dernière modif. March 04 2026 15:51:02.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 90a7c47c679f3b760ec96586e3bc75fa utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **12886** du fichier; voici le contexte :

```
FUlRJRklDQVRFLS0tLS0K';
        $script = <<<'EOT'

error_reporting(-1);
$info = openssl_x509_parse(base64_decode('%s'));
var_dump(PHP_VERSION, $info['issuer']['emailAddress'], $info['validFrom_time_t']);

EOT;
```

22. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/tgeoip/vendor/composer/ca-bundle/res/cace

(211.51K) (Date dernière modif. March 04 2026 15:51:02.)

Attention Les auteurs de virus utilisent parfois le codage "en e7cf471ba7c88f4e313f492a76e624b3 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 **50198** du fichier; voici le contexte :

```
CzAJBgNVBAYTAlVTMRAw
DgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxTdGFyZmllbGQg
VG">VjaG5vbG9naWVzLCBJbmMuMTIwMAYDVQQDEylTdGFyZmllbGQgUm9vdCBDZXJ0aWZpY2F0ZSBB
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 **51709** du fichier; voici le contexte :

```
CzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxT
dGFyZmllbGQgVG">VjaG5vbG9naWVzLCBJbmMuMTswOQYDVQQDEzJTdGFyZmllbGQgU2VydmljZXMg
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 **61021** du fichier; voici le contexte :

```
0Q0EyMB4XDTA5MDUyOTA1MDAzOVoXDTI5MDUyOTA1MDAzOVowXTELMAkGA1UEBhMC
SlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF">N5c3RlbXMgQ08uLExURC4xJzAlBgNVBAsTHlNlY3Vy
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 **116502** du fichier; voici le contexte :

```
gAwIBAgIQIdbQSk8lD8kyN/yqXhKN6TANBgkqhkiG9w0BAQ0FADCBgDELMAkGA1UE
BhMCUEwxIjAgBgNVBAoTGVVuaXpldG8gVG">VjaG5vbG9naWVzIFMuQS4xJzAlBgNVBAsTHkNlcnR1
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 **216059** du fichier; voici le contexte :

```
0Q0ExMB4XDTE2MDYxNjA1MTUyOFoXDTM4MDExODA1MTUyOFowYTEL
MAkGA1UEBhMCSlAxJTAjBgNVBAoTHFNFQ09NIFRydXN0IF">N5c3RlbXMgQ08uLExURC4xKzApBgNV
BAMTIlNlY3VyaXR5IENvbW11bmljYXRpb24gRUNDIFJvb3RDQTEwdjAQBgcqhkjOPQIBBgUrgQQA
```

23. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/tgeoip/tgeoip.php *(2.86K)*

(Date dernière modif. March 04 2026 15:51:02.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 6c8b4a40dac250fc985f50ce43477fbf utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **2360** du fichier; voici le contexte :

```
msgType = 'error';
                    $msg = $result;
                }

                $return = base64_decode($this->app->input->get->getBase64('return', nul

                $this->app->enqueueMessage($ms
```

24. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/fields/smarttagsbox.php

(4.41K) (Date dernière modif. March 04 2026 15:50:55.)

Danger Ce mot est un mot ayant été encodé en base64 et ebc327d75af19b203852277503e91fd5 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 **4293** du fichier; voici le contexte :

```
'{post.YOUR_KEY}' => Text::_('NR_POST_DATA'),
                    '{cookie.YOUR_KEY}' => Text::_('NR_COOKIE')
                ]
            ]
        ]);

        // Render box layout
        $layout = new F
```

25. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/fields/tffileupload.php

(6.74K) (Date dernière modif. March 04 2026 15:50:55.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 77bb168336c2cb43035a8849ae42fd80 utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **4666** du fichier; voici le contexte :

```
UPLOAD_ERROR_INVALID_FILE');
                }

                // Delete the file
                try {
                        return ['success' => File::delete(base64_decode($filename))];
                } catch (\Throwable $th)
                {
                        $this->uploadDie($th->getMessage());
                }
    }
```

26. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/fields/nrinlinefileupload.php

(3.40K) (Date dernière modif. March 04 2026 15:09:28.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef b38a3e96a183110b8b5b779351457204 utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **1924** du fichier; voici le contexte :

```
OLDER_MISSING')
                        ]);
                        jexit();
                }

                // ensure we can decode its value
                if (!$upload_folder = base64_decode($upload_folder))
                {
            echo json_encode([
                                'error' => true,
                                'response' => Text::_(
```

27. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Countries.php

(48.07K) (Date dernière modif. March 04 2026 15:50:55.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 5e25c8bc688781a44391f50710b5fd21 utilisé est néanmoins suspect.
Signature : **chell**
Trouvé en position **5505** du fichier; voici le contexte :

```
ome and Principe",
                'SA' => "Saudi Arabia",
                'SN' => "Senegal",
                'RS' => "Serbia",
                'SC' => "Seychelles",
                'SL' => "Sierra Leone",
                'SG' => "Singapore",
                'SK' => "Slovakia",
                'SI' => "Slovenia",
```

28. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/CacheManage

(2.81K) (Date dernière modif. March 04 2026 15:50:55.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé c0fe9eb85f06446b35ae0f4bf4371a2f est néanmoins suspect.
Signature : **hell**
Trouvé en position **1274** du fichier; voici le contexte :

```
a hash's value
         *
         *  @param   string  $hash  The hash string
         *  @param   string  $clone Why the_hell we clone objects here?
         *
         *  @return  mixed          False on error, Object on success
         */
        pub
```

29. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Visitor.php

(2.23K) (Date dernière modif. March 04 2026 15:50:55.)

Danger Ce mot est un mot ayant été encodé en base64 et 34173b74cd859aa63f8d5d34ba20e265 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 **497** du fichier; voici le contexte :

```
ookie used to identify that a visitor is persistent.
         *
         * @var  string
         */
        private $persistent_cookie_name = 'tvp';

        /**
         * Represents the maximum age of the visitor's persistent cookie in seconds.
```

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 **684** du fichier; voici le contexte :

```
cookie in seconds.
         *
         * Default value set to 1 year.
         *
         * @var  int
         */
        private $persistent_cookie_expire = 31536000;

        /**
         * The name of the cookie used to identify that a visitor is new.
         *
```

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 **828** du fichier; voici le contexte :

```
e of the cookie used to identify that a visitor is new.
         *
         * @var  string
         */
        private $session_cookie_name = 'tvs';

        /**
         * Represents the maximum age of the visitor's session cookie in seconds.
         *
```

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 **1014** du fichier; voici le contexte :

```
ookie in seconds.
         *
         * Default value set to 20 minutes.
         *
         * @var  int
         */
        private $session_cookie_expire = 1200;

        /**
         * The Cookies instance.
         *
         * @var  object
         */
        private $cookies;

        pub
```

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 **1611** du fichier; voici le contexte :

```
)
        {
                if ($this->isNew())
                {
                        // Update the session cookie
                        $this->cookies->set($this->session_cookie_name, 1, time() + $th
                }

                // Update the persistent coo
```

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 **1651** du fichier; voici le contexte :

```
ate the session cookie
                        $this->cookies->set($this->session_cookie_name, 1, time() + $th
                }

                // Update the persistent cookie
                $this->cookies->set($this->persist
```

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 **1761** du fichier; voici le contexte :

```
pire, '/', '', true);
                }

                // Update the persistent cookie
                $this->cookies->set($this->persistent_cookie_name, 1, time() + $this->p
        }

        /**
         * Checks whether the
```

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 **1804** du fichier; voici le contexte :

```
persistent cookie
                $this->cookies->set($this->persistent_cookie_name, 1, time() + $this->p
        }

        /**
         * Checks whether the user is considered new.
         *
         * A user is
```

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 **2170** du fichier; voici le contexte :

```
*
         * @return  bool
         */
        public function isNew()
        {
                $tvp = $this->cookies->get($this->persistent_cookie_name);
                $tvs = $this->cookies->get($this->session_cookie_name);

                return (!$tvp && !$tvs) || $tvs
```

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 **2228** du fichier; voici le contexte :

```
vp = $this->cookies->get($this->persistent_cookie_name);
                $tvs = $this->cookies->get($this->session_cookie_name);

                return (!$tvp && !$tvs) || $tvs;
        }
}
```

30. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Integrations/Dr

(7.04K) (Date dernière modif. March 04 2026 15:50:55.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef b50ea029fb6a4fa37b0ff534e3b976bb utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **3735** du fichier; voici le contexte :

```
return true;
        }

        /**
         * Assign a Subscriber to a Campaign
         *
         *  https://developer.drip.com/?shell#subscribe-someone-to-a-campaign
         *
         * @return  void
         */
        private function assignSubscriberToCam
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **4533** du fichier; voici le contexte :

```
}

        /**
         * Returns whether the subscriber is in a campaign
         *
         * https://developer.drip.com/?shell#list-all-of-a-subscriber-39-s-campaign-sub
         *
         * @return  bool
         */
        private function
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **5199** du fichier; voici le contexte :

```
ign;

        }

        /**
         * Returns the ID of the subscriber from email
         *
         * https://developer.drip.com/?shell#fetch-a-subscriber
         *
         * @return  string
         */
        private function getSubscriberIdFromEmail($email)
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **5932** du fichier; voici le contexte :

```
: array();
        }

        /**
         *  Returns all available Drip campaigns
         *
         *  https://developer.drip.com/?shell#list-all-campaigns
         *
         *  @return  array
         */
        public function getLists()
        {
                $data = $this->get
```

31. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Conditions/Cor

(22.67K) (Date dernière modif. March 04 2026 15:50:55.)

Danger Ce mot est un mot ayant été encodé en base64 et 56d029d15d649fc846eb36c462c79103 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 **22847** du fichier; voici le contexte :

```
],
                    'Cookie' => [
                        'title' => Text::_('NR_COOKIE'),
                        'desc' => Text::sprintf('NR_COOKIE_CONDITION_DESC', $product)
```

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 **22909** du fichier; voici le contexte :

```
'title' => Text::_('NR_COOKIE'),
                        'desc' => Text::sprintf('NR_COOKIE_CONDITION_DESC', $product)
                    ],
                    'PHP' => [
```

32. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Conditions/Mig

(6.42K) (Date dernière modif. March 04 2026 15:50:55.)

Danger Ce mot est un mot ayant été encodé en base64 et 213191d308bf99786394a80d4437fa17 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 **4489** du fichier; voici le contexte :

```
}

                $operator = $operatorMap[$value];

                $params->set('assign_cookiename_param_operator', $operator);

                $value = $params->get('assign_cookiename_param_na
```

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 **4576** du fichier; voici le contexte :

```
->set('assign_cookiename_param_operator', $operator);

                $value = $params->get('assign_cookiename_param_name');
            }

            if ($newName == 'Pageviews')
            {
```

33. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Executer.php

(9.01K) (Date dernière modif. March 04 2026 15:50:55.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 35ad7bc8454207484282328637968ba6 utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1368** du fichier; voici le contexte :

```
,
                'unlink',
                'rmdir',
                'dl',
                'escapeshellarg',
                'escapeshellcmd',
                'exec',
                'passthru',
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1402** du fichier; voici le contexte :

```
'rmdir',
                'dl',
                'escapeshellarg',
                'escapeshellcmd',
                'exec',
                'passthru',
                'proc_close',
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell_exec**
Trouvé en position **1541** du fichier; voici le contexte :

```
'passthru',
                'proc_close',
                'proc_open',
                'shell_exec',
                'symlink',
                'system',
                'pcntl_exec',
```

34. /home/vx3xycwr/economie.pennes-mirabeau.org/plugins/system/nrframework/NRFramework/Cache.php

(2.69K) (Date dernière modif. March 04 2026 15:50:55.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 7282393a1d6a0866513a0e9ab237a666 utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **879** du fichier; voici le contexte :

```
rns hash value
         *
         *  @param   string  $hash  The hash string
         *  @param   string  $clone Why the hell we clone objects here?
         *
         *  @return  mixed          False on error, Object on success
         */
        sta
```

© Avonture Christophe 2013-2026 | *aeSecure QuickScan v.2.2.2* (https://github.com/AFUJ/quickscan/)