Guide de présentation

OFFICE-ANALYZE

Office Analyse

Ce que vous devez savoir

- Son objectif
- Sa conception
- Infection DOCX
- Son Guide d'utilisation

Objectifs

- Detection de malware
- Sortir toutes les métas-datas du fichiers
- Sortir tout les hyperliens visible du fichier
- Sorti toutes les images ainsi que les hyperliens liés
- Désactive & copie la macro d'un fichier
- Docx,Dotm,Docm

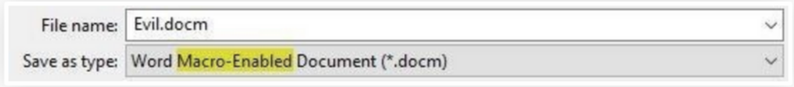
Sa conception

1. **Accéder aux méta-datas**
2. **Extraction des méta-datas**
3. **Extraction/Détection des hyperliens**
4. **Extraction/Détections des images + hyperliens**
5. **Désactivation/ Extraction des macros**

Selon la méthode WaterFall

Infection .DOCX

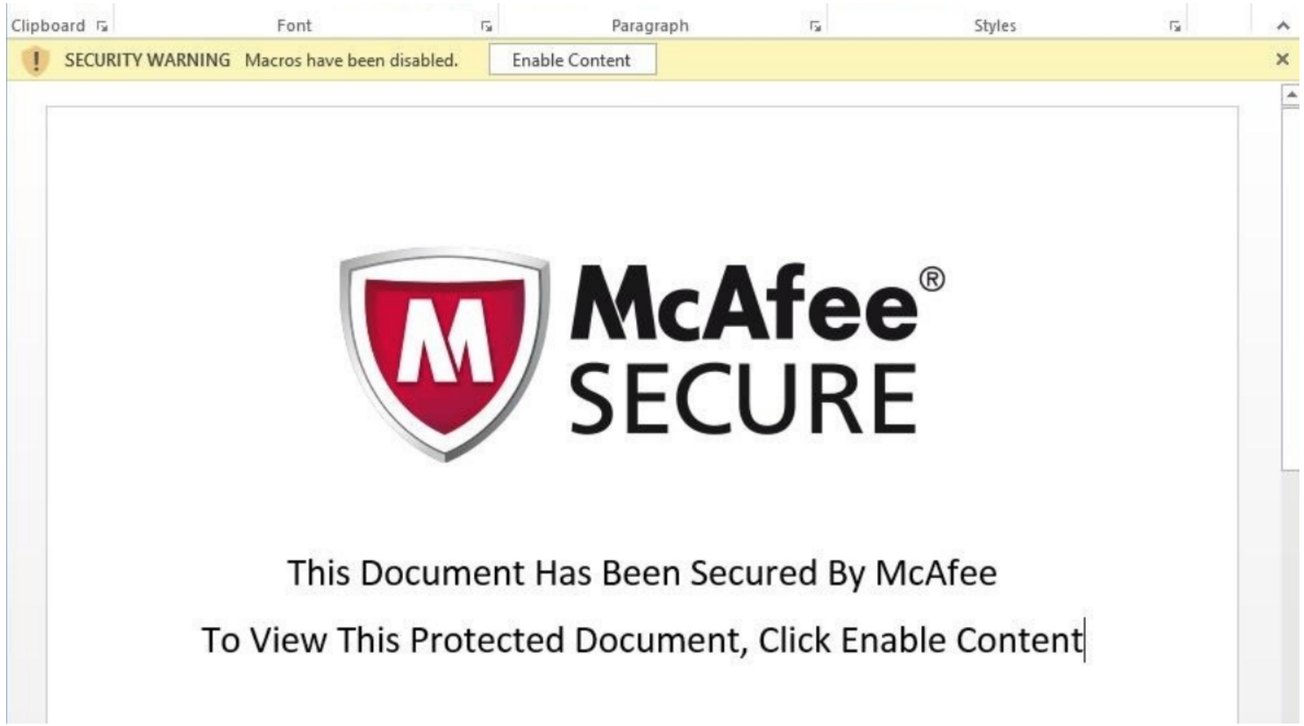
To add it to a document, open Microsoft Word and create a new document called *Evil.docm*. Make sure "Macro-Enabled" is selected from the drop-down menu.



Next, on the View tab, click on "Macros" on the right-hand side.

It will prompt you to create a new macro, so type *Auto_Open* and click "Create." Also, make sure that the drop-down menu next to "Macros in:" has the name of your document selected, and not "All active templates and documents," because it may get confusing.

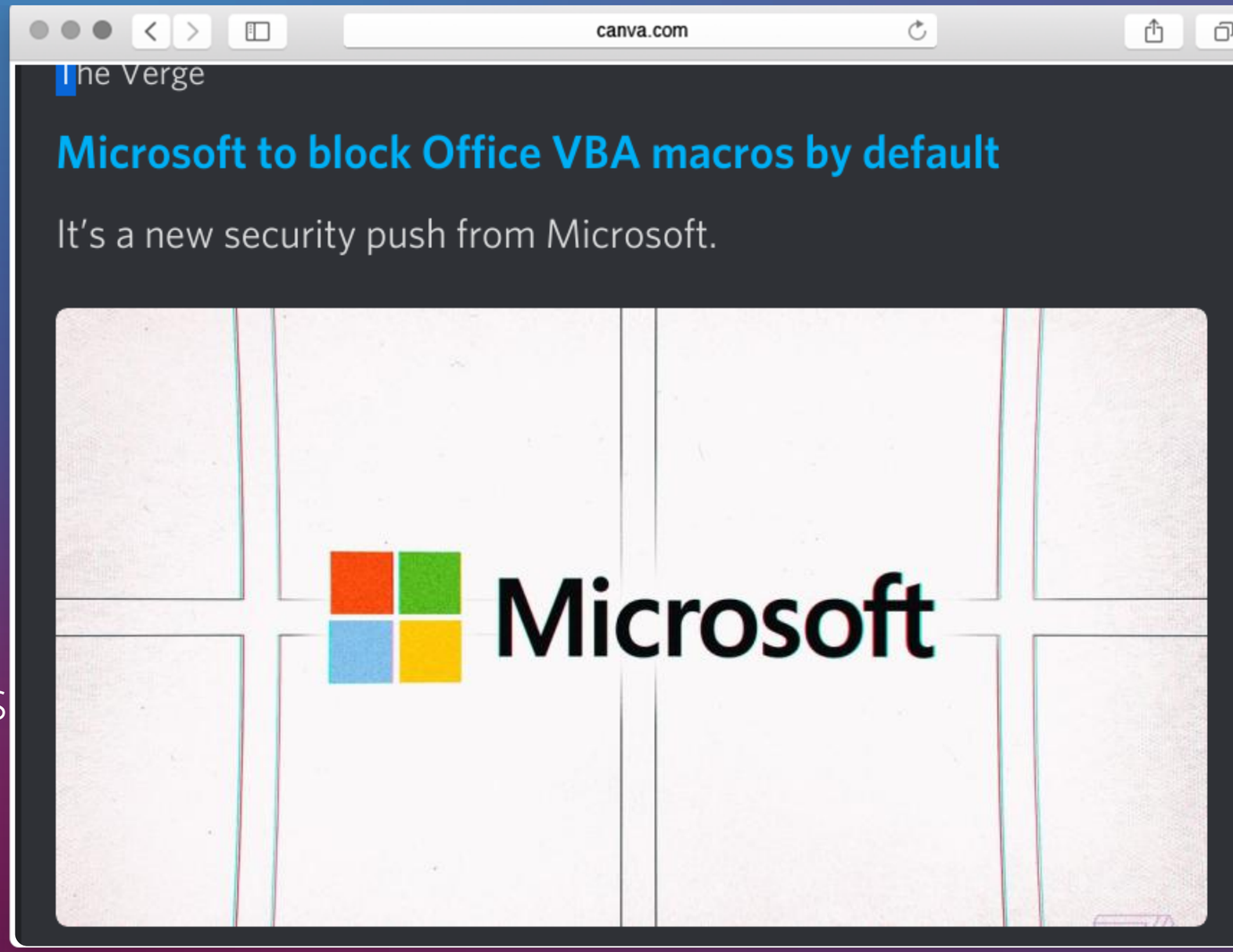
- Créer une macro et l'enregistré dans un docm
- Changer le template utilisé dans le fichier XML pour le .docx par le fichier .docm



Nous avons rencontré des difficultés

Microsoft décide de bloquer par défault les macros dans les .DOCX

Source



```
#define SHELLSCRIPT "\
#!/bin/bash                                  \n\
#pwd                                         \n\
echo \"Copie du fichier\"                    \n\
file_doc=`ls *.doc *.docx`                   \n\
for i in $file_doc                           \n\
    do                                           \n\
        cp $i general.zip                            \n\
    done                                         \n\
echo \"copie terminé\"                       \n\
unzip general.zip -d general\
"

#define SHELLSCRIPT2 "\
#!/bin/bash   \n\
cd .\.\   \n\
cd \Projet_C\n\
rm -Rf general.zip\n\
rm -Rf general\n\
"
```

Accéder aux méta-datas

On va compresser le fichier puis le décompresser afin de pouvoir accéder aux métas-datas

Extraction des métas-datas

Sorti terminal de l'extraction des métas-datas

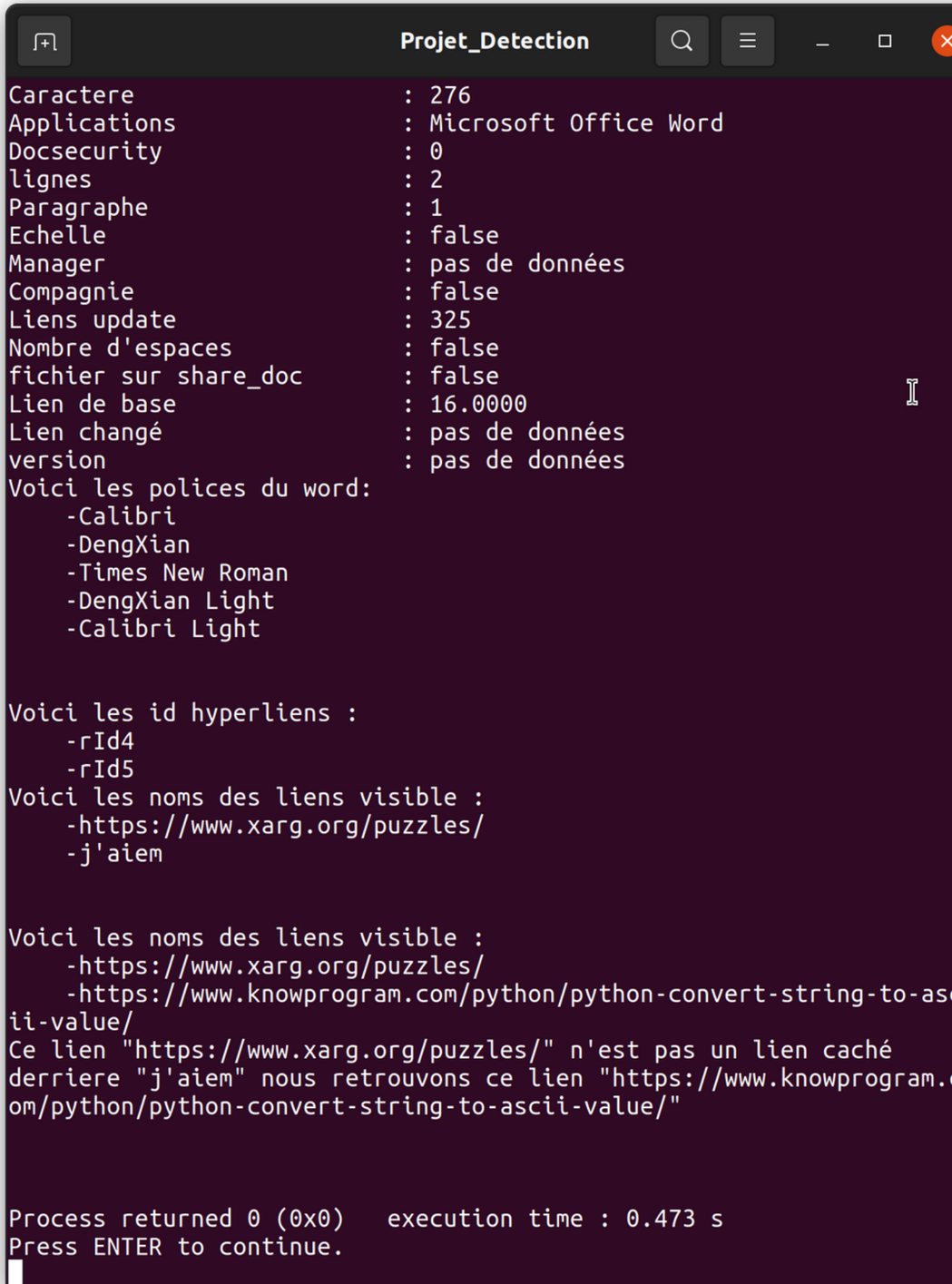
Situé dans :
/generale/docProps/app.xml ou core.xml
Les police elle utilisé sont situé :
/genral/word/fontTable.xml

Extraction/Détection des hyperliens

Sorti terminal de l'extraction des hyperliens

Situé dans :
/generale/word/_rels/document.xml.rels

- Affiche les hyperliens visible
- Affiche les liens des hyperliens
- Détection si le liens est un lien caché ou pas



Extraction/Detections des images + hyperliens

Sorti terminal de l'extraction des métas-datas

Situé dans : /generale/word/_rels/document.xml.rels

```
Projet_Detection
Titre                          : pas de données
Sujet                          : pas de données
Créateur                       : XU William
Descriptions                   : pas de données
Dernier ayant modifie2         : XU William
Nombre de revisoins            : 2
Création du doc                : pas de données
Derniere modification          : pas de données
Categorie                      : pas de données
Langue                         : pas de données
Template                       : Normal.dotm
Nombre de fois ouvert          : 4
Pages                          : 1
Mots                           : 0
Caractere                      : 4
Applications                   : Microsoft Office Word
Docsecurity                    : 0
lignes                         : 1
Paragraphe                     : 1
Echelle                        : false
Manager                        : pas de données
Compagnie                      : false
Liens update                   : 4
Nombre d'espaces               : false
fichier sur share_doc          : false
Lien de base                   : 16.0000
Lien changé                    : pas de données
version                        : pas de données
Voici les polices du word:
    -Calibri
    -DengXian
    -Times New Roman
    -DengXian Light
    -Calibri Light


donc = image2.png = https://www.youtube.com/watch?v=ru4ZWOSOsPM
donc = image1.png = https://openclassrooms.com/forum/sujet/codebloc
p-67632

Process returned 0 (0x0)   execution time : 0.182 s
Press ENTER to continue.
```

Avant suppréssion

document.xml.rels — general

```
2  <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/
   relationships/settings" Target="settings.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><
   Relationship Id="rId1" Type="http://schemas.microsoft.com/office/2006/relationships/vbaProject" Target="vbaProject.bin"/><Relationship Id="rId6" Type="
   http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/
   officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings
   " Target="webSettings.xml"/></Relationships>
```

Après suppréssion macro

document.xml.rels — general

```
2  <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/
   relationships/settings" Target="settings.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><
   Relationship Id="rI6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship Id="rId5" Type="
   http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/
   officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/></Relationships>
```

Supprimer la relation qu'il y avait
avec le fichier vbaProject.bin qui
désactive la macro

Guide d'utilisation

- Suffit de placer le fichier que l'on veut analyser dans le fichier du programme
- Puis de lancer le programme
- Si une macro est détecté elle est automatiquement supprimé
- L'utilisateur à un retour sur les liens susceptible d’être malveillant

Merci de nous avoir écouté

Avez-vous des questions ?

HAMRENE Liticia
Boissel Jules
William Xu
Adrien Dusserre