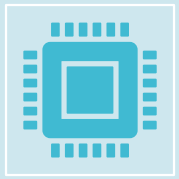
TP1– Respect des bonnes pratiques

SIO1

B3 Cybersécurité

Les fichiers dangereux

Certaines des pièces jointes que vous recevez par mail peuvent contenir un fichier malveillant

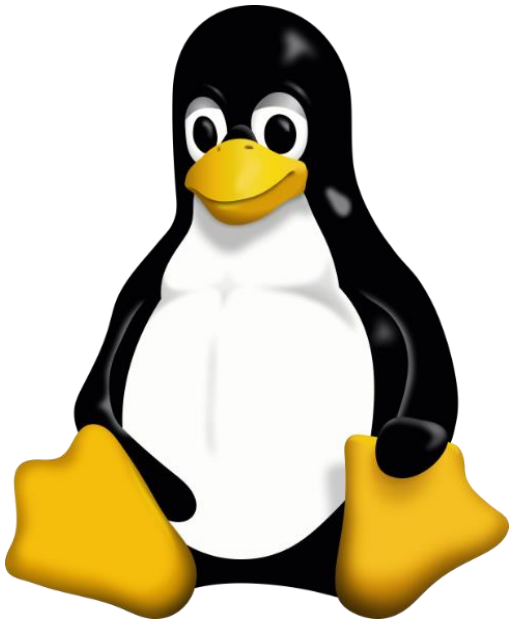


Ce fichier malveillant, aussi appelé malware peut conduire à un arrêt de votre entreprise

Voyons comment distinguer les fichiers dangereux pour s'en protéger

Les fichiers dangeureux pour un ordinateur

Pour un ordinateur il existe plusieurs formats de fichiers qui représentent un danger



Les fichiers exécutables

Un fichier exécutable est un fichier contenant un programme qui peut être exécuté par le système d'opération. Un hacker peut ainsi caché dans le fichier exécutable un programme néfaste pour l'entreprise.

- **Windows**

.exe

.com

.bat

.cmd

.msi

.dll

.sys

- **Linux**

.sh

.bin

.run

.rpm

.deb

.elf

- **Mac**

.app

.dmg

.pkg

Les Scripts

Un fichier script est un fichier qui exécute une commande. Ils peuvent représenter un risque pour votre entreprise si un malware (programme malveillant) y est caché.

- **Windows**

.vbs

.js

.ps1

.wsf

.hta

.py

- **Linux**

.sh

.py

.pl

.rb

.php

- **Mac**

.vbs

.js

.ps1

.wsf

.hta

Les fichiers Macros

Vous les connaissez sous le nom de la suite office. On y retrouve les fichiers Word, Excel ou encore Powerpoint. Ces fichiers ont des scripts incorporés qui peuvent être détourné pour une utilisation malveillante.

Windows/Linux/Mac

.doc/.docx

.xls/.xlsx

.ppt/.pptx

.odt/.ods/.odp

Les Fichiers d'archive

Les fichiers archives sont des fichiers qui ont étaient compressé par un algorithme de compression pour gagner de la place. Un hacker peut y dissimuler un malware à l'intérieur.

Windows/linux/mac	
.zip	
.rar	
.7z	
.iso	

Fichiers multimédias Windows/Linux/MacOs

Il s'agit des fichiers d'images, de vidéos ou d'extrait audio. Le logo de votre entreprise est enregistré sous forme de fichier image.

Moins dangereux car les attaquent nécessitent des failles dans les lecteurs multimédias.

Images : .png ; .gif ; .jpg

Vidéos : .mp4 ; .avi ; .mkv ; .3gp

Audios : .mp3 ; .wav

Fichiers Web

Il s'agit de fichiers qui contiennent des scripts pour afficher ou diffuser le contenu d'Internet. Ils souffrent ainsi des mêmes problèmes que les fichiers scripts.

Windows/Linux/Mac

.htlm

.htm

.php

.asp

iOS

Les fichiers dangeureux sur Android/IOS

Fichiers d'installation

Ceux sont eux qui permettent d'installer une application sur votre téléphone ou votre tablette. Ils peuvent être détourné pour installer un malware à la place.

Pour Android :

.apk

.dex

Pour IOS :

.ipa

Fichiers multimédias (même chose que sous Windows)

Images : .png ; .gif ; .jpg

Vidéos : .mp4 ; .avi ; .mkv ; .3gp

Audios : .mp3 ; .wav

Fichiers Macros et fichiers compressés :

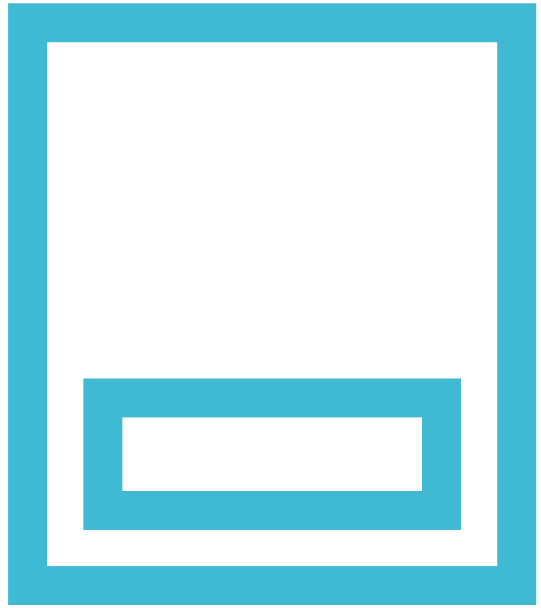
(même chose que sous PC)

Fichiers Macro	Fichiers Compressé
.doc/.docx	.zip
.xls/.xlsx	.rar
.ppt/.pptx	.7z
.odt/.ods/.odp	.iso

Les Fichiers Script et fichiers Web

On retrouve certains des fichiers dangereux sous PC :

.htlm ; .htm ; .js



Des Formats particulièrement dangereux

Tous les fichiers que vous pouvez recevoir par pièces jointes constituent ainsi une menace.

Certains fichiers sont cependant plus couramment utilisés par les hackers :

- Les fichiers Macro car ils sont souvent présents dans le milieu de l'entreprise
- Les fichiers exécutables et de script car ils permettent d'exécuter directement du code malveillant sur la machine une fois lancé

Des formats plus sûr

Certains formats de fichiers représentent une menace faible voir pas de menace du tout

Le format .pdf et .txt sont sûr car ils ne contiennent pas de script

Les formats multimédias sont relativement sûr car ils ne peuvent pas exécuter du code. Mais le logiciel de visualisation doit être maintenu à jours pour empêcher toutes vulnérabilité. Rester vigilant

Les mesures de sécurité essentielle

Mesure 1 : Vérifier les sources : Vérifié l'émetteur du mail quand vous ouvrez une pièce jointe, si vous avez un doute sur la fiabilité de l'émetteur ne touchez pas au pièces jointes

Mesure 2 : Mettre à jour régulièrement les logiciels/Système d'exploitation : Les hackers utilisent des failles dans ses systèmes pour pouvoir infecter votre machine/entreprise. Celles-ci sont corrigé à chaque mise à jour.

Mesure 3 : Analyser les fichiers télécharger avec l'antivirus, même quand le fichier provient d'une source sûr. De plus soyez attentifs aux extensions de fichiers (correspond -elle au bon format (pas de .exe pour une image par exemple))

Mesure 4 : Désactiver les macros de la suite office

Mesure 5 : Sauvegarder régulièrement vos données, ce qui permet de limiter les dommages lors d'une attaque

Identifier les sources sûrs

Voici quelques conseils pour connaître ou télécharger ou de qui recevoir des fichiers sûr.

Sites officiels des éditeurs de logiciels : Ex Microsoft store

Boutiques d'applications officielles : Pour IOS Apple Store

Mails de confiance : De personnes ou de sociétés que vous connaissez

Pourquoi se protéger des malwares ?

Cas concret du malware Emotet

Dans un premier temps un hacker vous envoie un mail avec pour pièce jointe un document de la suite office.

Une fois les fichiers Word ou Excel ouvert et les Macros activé, le code des macros se connecte à un serveur pour télécharger le malware Emotet

Le malware se propage alors dans le réseau de l'entreprise et télécharge d'autres malware qui vont chiffrer les données et rendre inutilisable tout le réseau informatique

C'est-ce qui est arrivé à la ville Allentown en Pennsylvanie ce qui lui a couté **plus d'un million de Dollars**.

Une telle attaque peut interrompre l'activité de votre entreprise pendant plusieurs semaines et la conduire à la faillite, d'où l'importance d'adopter les mesures de sécurité essentielle listé précédemment.