Ugo Bemben 2022-2024

TP1_Respect des bonnes pratiques

1) Format de fichier dangereux pour WINDOWS

a) Programme

.EXE - Un fichier de programme exécutable.
.PIF – C'est un format de fichier que Windows traitera de la même manière que .EXE
.APPLICATION – à faire des attentions à ce type de fichier car c'est un Click Once
.JAR – le .jar permet d'exécuter un code javascript
.MSI – et le plus utilisé pour installer un virus

b) Script

.bat – A FAIRE TRES ATTENTION CAR IL PEUT EXECUTER UNE LISTE DE COMMANDE SUR VOTRE PC
.cmd – fonctionne de la même manière que le .bat donc à faire attention aussi
.js – permet de lancer des lignes de commande a javascript sur votre ordinateur

Bien sûr il existe plein d'autre extension dangereuse met celle écrite si dessous sont le plus fréquente.
A faire également attention à l'extension cacher par exemple « Image.png.EXE » cela peut être fait avec tout type d'extension. Il ne faut aussi faire attention en .rar souvent si le dossier a un mot de passe il contient souvent un virus.

2) Format de fichier dangereux pour LINUX

Les formats de fichier dangereux sur linux sont pratiquement les mêmes que sur Windows.
Comme sur Windows il faut faire attention principalement au « .EXE, .ISO,.PIF,.JAR,.BAT, .CMD ».
Et comme sur Windows il faut faire attention au fichier cacher par exemple « Image.png.EXE ».

3) Format de fichier dangereux pour MAC

Sur mac il a pas mal de fichier de format de fichier dangereux parmi les plus dangereux on retrouve :

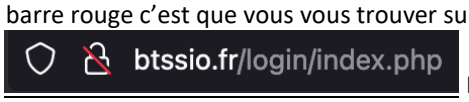
.dmg - le .dmg et le principale format d'installation MAC

.jpeg – un format d'image met peut contenir des lignes de code cacher parmi les milliers d'autre

Ensuite il a les formats de base qu'on retrouve sur Windows et Linux

4) Il y a des formats de fichier plus dangereux que d'autre par exemple .exe car il permet d'exécuter un programme sur votre pc sans connaitre réellement ce qu'il contient ce qui correspond au .dmg sur mac

5) Pour savoir si la sources sur laquelle vous vous trouvez actuellement et plus sûr qu'une autre, un indice qui peut vous aider et le Cadenas dans la barre de recherche si il est fermé ou si il n'a pas de barre rouge c'est que vous vous trouver sur un site que et censé être sécurisé



Par exemple ce site n'est pas sécurisé donc vous changer de site pour en trouver un plus sure

6) Pour vous protéger les maximums d'un rançongiciel il faut mettre vous donner sensible comme (photo de carte identité, carte de sécurité social, compte en banque) dans une clé USB que vous branchez sur votre pc que quand vous en avez l'utilité. Il faut aussi faire attention au mail que vous recevez par exemple si on vous dit que vous avez gagné un iPhone 13 PRO MAX a 1 euros il ne faut pas cliquer on ne vit pas dans le monde des bisounours. Si vous recevez un message bibard par exemple votre colis est arriver alors que vous n'attendez rien ne cliquer pas sur ce lien ceci et surement une arnaque, n'oublié surtout pas de mettre votre ordinateur a jour et de prendre un anti-virus comme ESET par exemple, SI malgré tout vous parvenez a être infecté surtout ne payez pas la rançons dans tous les cas il est trop tard il ont déjà vous donnée.

7) J'imagine que vous me prenez pour un parano mais il a eu des faits par exemple vous travailler dans une entreprise vous recevait un mail pour vous connecter à votre panel de gestion et le hacker a accès a vos identifiant donc a accès a toute l'entreprise et a cause de vous venez compromettre toute votre entreprise et vos mail et peut être même le mail de vos client. A cause de cette erreur vos aller sûrement vous faire virer.