TP1 : Respect des bonnes pratiques

Florentin Bracq- -Flabat
BTS SIO 1

Travail à réaliser :

1) Présentez à vos utilisateurs les formats de fichiers qui peuvent être dangereux sur un PC (Windows, Linux, Mac), sur un smartphone ou une tablette (Android, IOS).

Sous Windows :

Les fichiers pouvant être dangereux sont très souvent les fichiers exécutables (.exe), ces fichiers apportent la plupart du temps des modifications au système d'exploitation. Ces fichiers sont souvent utilisés pour installer des programmes.

Les fichiers en .msi peuvent également être dangereux, ces fichiers utilisent le programme Windows Installer pour s'installer, ces fichiers peuvent être dangereux surtout s'ils contiennent un programme malveillant.

Les fichiers plus utilisés en .docx, .xlsx, .pptx ou encore les .pdf peuvent égalent être dangereux quand ils sont inconnus, ils peuvent contenir un programme malveillant.

Les fichiers .bat sont également dangereux, ces fichiers sont capables d'exécuter des commandes dans le terminal, s'il a les droits d'administration il serait capable de détruire votre système d'exploitation.

Les fichiers .reg sont dangereux parce qu'ils peuvent apporter des modifications au registre de votre système, si des modifications apportées par ce type de fichiers sont trop importantes, cela peut aller jusqu'à casser votre système.

Les fichiers images en .png .jpg où .gif, peuvent également être également dangereux, ils peuvent contenir du code malveillant, des malwares ou des virus.

Les fichiers musicaux tels que les fichiers en .mp3 peuvent également être dangereux surtout quand on ne connaît pas sa provenance.

Les fichiers vidéo tels que les fichiers en .mp4 .avi etc, peuvent également être dangereux tout comme les fichiers musicaux quand on ne connaît pas la provenance du fichier

Sous Linux :
Les fichiers en .deb peuvent être dangereux, ces fichiers sont souvent utilisés pour installer des programmes en dehors des bibliothèques de votre distribution.

Les fichiers .gz peuvent être dangereux sous linux, ces fichiers sont des archives et peuvent contenir un programme malveillant.

Les fichiers .tar peuvent également être dangereux sous linux, tout comme les fichiers en .gz ce sont des archives, une fois l'archive décompressée on peut obtenir un fichier exécutable inconnu, il faut donc prendre des précautions.

Sous Mac :
Les fichiers en .txt peuvent être dangereux sous Mac, ils peuvent exploiter une faille de sécurité dans l'éditeur de texte pour essayer d'apporter des modifications à la machine.

Les fichiers .dmg peuvent assent souvent présenter un danger pour le système d'exploitation, c'est un format de fichier image disque qui permet l'installation d'une application Mac à l'aide d'un double-clic.

Les fichiers en .pkg sont des fichiers paquet qui contiennent généralement des scripts utilisés pour effectuer une installation, ils peuvent être dangereux parce qu'ils pourraient exécuter des scripts pouvant exécuter d'autres actions pour altérer le fonctionnement du système d'exploitation.

Les fichiers en .app peuvent également représenter une menace, par qu'ils constituent les applications en tant que telles. Ils peuvent également fonctionner depuis n'importe quel emplacement.

Sous Android :
Les fichiers .apk peuvent présenter un danger sous Android, ces fichiers permettent d'installer une application manuellement, quand elle n'est pas disponible depuis le Play store, ou alors une application qui est en cours de développement peut parfois être disponible au début uniquement sous forme d'un fichier .apk

Les fichiers en .zip ou encore .rar sont des fichiers d'archive, il peut être une menace sur Android, mais pas seulement. Ils peuvent être dangereux sur d'autres systèmes d'exploitation, tels que Windows ou MacOS.
Sur iOS :

Les fichiers en .ipa sont des paquets sui permettent d'installer des applications sur iOS ,il peuvent également être dangereux parce qu'il pourraient installer une application malveillante.

2) Déterminez si les formats de fichiers sont plus dangereux que d'autres. Argumentez.

Les formats de fichiers les plus dangereux sont les fichiers en .exe on les trouve assez souvent sur Windows, ces fichiers sont parfois dangereux, contiennent parfois des logiciels malveillants, qui sont bien plus répandus sur Windows que sur les autres systèmes d'exploitation sur PC qui sont moins utilisés.

Les fichiers au format .msi peuvent également être dangereux tout comme les fichiers en .exe, ces fichiers sont des packages pour Windows, ils peuvent installer des programmes et apporter des modifications au système d'exploitation. Ce format de fichier est un peu moins répandu que les .exe, c'est donc pour cela que j'ai choisi de placer cette extension de fichier en 2ème place.

Tous les fichiers permettant d'installer des applications, sur Android, iOS où tout autre système d'exploitation (.apk, .ipa), peuvent être dangereux pour les appareils mobiles tels que les téléphones ou les tablettes. Ces fichiers sont des package pour installer des applications sur les systèmes d'exploitation mobiles.

Les fichiers d'archives (.rar, .zip etc…), sont dangereux pour tous les systèmes d'exploitation, au moment où vous décompressez le fichier, il peut y avoir un malware dedans qui peut infecter le système d'exploitation.

Tous les fichiers documents, images, musiques et vidéos, peuvent contenir des malwares surtout quand on ne sait pas d'où ils viennent. J'ai choisi de placer ces types de fichiers en dernière place parce qu'en général ces fichiers sont moins souvent infectés.

3) Y a t-il des sources plus sûres que d'autres ? Explicitez avec des exemples.

Quand on prend l'exemple pour télécharger un fichier en .exe où .msi, pour installer un logiciel, dans un premier temps il faut se renseigner sur l'éditeur du logiciel afin de pouvoir télécharger le fichier d'installation depuis le site officiel de l'éditeur, il faut éviter les sites alternatifs de téléchargements.

Pour les autres fichiers tels que les documents, images, archives etc… Faites confiance de préférence aux personnes que vous connaissez physiquement. Éviter le téléchargement de documents inconnus en ligne, pour éviter d'être

infecter, hormis si vous utiliser un espace de stockage en ligne, ou si une personne que vous connaissez.

4) Comment allez-vous inciter vos utilisateurs à se protéger des menaces informatiques, dans notre cas d'un rançongiciel.

Dans un premier temps, il pourrait être possible de créer des affiches pour sensibiliser les utilisateurs, faire des interventions de sensibilisations, des spots pubs radio et télévision. Faire des démonstrations à petite échelle pour sensibiliser encore plus.

5) Vos utilisateurs vont certainement vous prendre pour un « parano ». Comment allez-vous démontrer que ces mesures peuvent être vitales pour le bon fonctionnement de l'entreprise ?

Il pourrait être possible de faire une démonstration d'une infection à but éducatif, pour pouvoir donner une idée aux utilisateurs du danger. Il faudrait expliquer aux utilisateurs pourquoi il faudrait limiter les clé USB, afin de pouvoir limiter les infections par clé USB et privilégier l'utilisation du cloud. Expliquer pourquoi il faut éviter d'ouvrir les pièces jointes dans les mails, et demander par exemple aux utilisateurs d'envoyer leurs documents en pièce jointe au format .pdf