Guide de bonnes pratiques pour éviter les Ransomwares

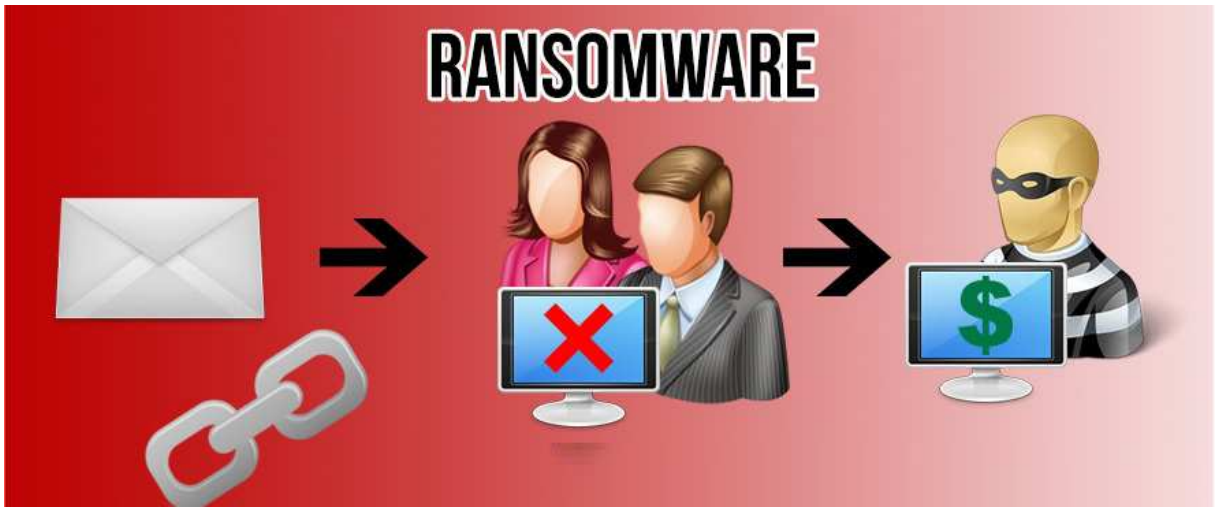
V1.0

Version	Date de la version	Modification apportée
1.0	04/04/2016	Premier draft

Document Public | Document Interne | Document Confidentiel | Document Top-Secret

Le Ransomware, ou rançongiciel est un logiciel malveillant, se diffuse principalement via des mails ou des supports amovibles infectés. Il prend en otage des données personnelles. Pour ce faire, un ransomware chiffre des données personnelles, ensuite il bloque l'accès de tout utilisateur à une machine, puis il demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui lui permettra de les déchiffrer.

Depuis le début de l'année ***2016***, les laboratoires spécialisés en sécurité informatiques ont signalé une augmentation importante des campagnes de « ***ransomwares*** » circulant sur le net. Ces menaces ont connu un grand développement soit au niveau de leurs ***techniques d'expansion*** ou encore leurs techniques de ***cryptage de données*** sur les disques durs.



Pour se protéger face à ces menaces, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

1. ***Sauvegarder vos données sensibles*** *sur des disques durs externes et n'oublier pas de les débrancher après la fin de l'opération de sauvegarde ;*

2. ***Créer,*** *périodiquement,* ***des points de restauration*** *pour récupérer les fichiers système en cas d'infection ; et veiller à les sauvegarder sur* ***Support externe****.*

3. ***Vérifier l'authenticité et la fiabilité des expéditeurs*** *avant la lecture de* ***chaque message reçu*** *par* ***e-mail*** *ou sur votre réseau sociaux (****Facebook, Twitter …)*** *et en cas de doute il ne faut* ***pas répondre, et aussi ne pas cliquer*** *sur les liens hypertextes ou les images qu'il contient et* ***surtout*** *si ces pièces sont au format* ***EXE, ZIP ou PDF ;***

4. *Pour les utilisateurs d'****Outlook****, on vous conseille de désactiver les générateurs d'aperçus de pièces jointes ;*

   https://support.office.com/fr-fr/article/Aper%C3%A7u-des-pi%C3%A8ces-jointes-a9b0921c-c1df-4922-aefb-26e9557de6fe

5. ***Vérifier*** *tous les messages portant des pièces jointes du type : .js (Javascript), .jar (java), .bat (Batch), .exe (fichier exécutable), .cpl (Control Panel), .scr (Screen saver), .com (COM file), .pif (Program Information File), .vbs (Visual Basic Script) ;*

6. ***Scanner*** *immédiatement* ***chaque périphérique USB*** *inséré dans votre machine et aussi* ***chaque fichier téléchargé*** *par votre solution antivirale de peur qu'il soit infecté ;*

7. *Désactiver* ***l'exécution automatique des macros*** *des suites bureautiques;* ***https://support.office.com/fr-fr/article/Activer-ou-d%C3%A9sactiver-les-macros-dans-les-documents-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12***

Nous rappelons que pour une navigation saine, nous vous recommandons de :

1. ***Mettre à jour*** *régulièrement votre* ***solution antivirale, activer la mise à jour automatique*** *de votre système et garder vos logiciels et plugin-in* ***à jour et surtout les points d'entrée des attaques*** *(Navigateurs, Java, Flash, Office, Acrobat…) ;*

2. Pour **se connecter à Internet, Utiliser** un **compte utilisateur** avec **des privilèges limités ;**

3. **Installer des Addons** dans votre navigateur web **pour vous renseigner sur la fiabilité des sites web visités** (Exemples: *Web Of Trust - WOT -,Netcraft) ;*

Procédure de désinfection de l'ordinateur

Si la machine infectée est en réseau, il faut l'isoler immédiatement (débrancher le câble réseau, ou couper l'accès WiFi) et essayer de restaurer le système à une date antérieure pour récupérer vos fichiers.

Il ne faut surtout pas payer la **rançon demandée** par **les pirates informatiques, puisque l'argent sera perdu** car rien ne garantit **que les données soient récupérées**.

Suivre la procédure suivante en mode sans échec :

1. *Redémarrer l'ordinateur, et avant le logo Windows, Taper sur la touche F8, un menu va apparaître.*
2. *Choisir alors le Mode sans échec avec prise en charge du réseau et appuyer sur la touche entrée du clavier*
3. *Une fois en mode sans échec: Supprimer les éléments malicieux via RogueKiller :*
   Lien de téléchargement du RogueKiller :
   https://www.ansi.tn/fr/pages/outils/kits_netoyage.html
4. *Après le pré-scan, lancer un Scan en cliquant sur le bouton Scan à droite. Le bouton Suppression devrait être dégrisé, Cliquer dessus afin de supprimer les éléments détectés.*
5. *Redémarrer votre PC , le ransomware devrait être éliminé.*

Si votre système est inaccessible (le ransomware bloque l'accès de tout utilisateur à votre machine) la seule solution qui s'offre à vous est de réparer la MBR et de réinstaller votre système d'exploitation.

En cas de difficulté lors de l'exécution des recommandations citées là-dessus, prière de nous contacter via téléphone : ***71 84 32 00*** *ou* ***71 84 20 90*** *ou par mail :* ***assistance@ansi.tn*** *ou bien par message facebook sur* ***www.facebook.com/ansitn****.*

Pour plus d'informations :

https://fr.wikipedia.org/wiki/Ransomware
https://www.microsoft.com/security/portal/threat/threats.aspx
https://blog.kaspersky.fr/petya-ransomware/5481/
http://www.bitdefender.fr/tech-assist/self-help/removing-police-themed-ransomware-malware.html
http://www.symantec.com/connect/fr/blogs/ransomware-how-stay-safe