Les Ransomwares ou Rançongiciels

Ce sont des logiciels malveillants redoutables qui, au moyen de techniques cryptographiques complexes, cryptent les données stockées dans la machine de leur victime (et même un disque amovible).

Une fois la machine prise en otage, les pirates contactent leurs victimes en demandant une rançon contre la "libération" de leurs données.

Quelles sont leurs cibles de choix ?

> Les comptes à privilèges (Administrateurs système)

Les administrateurs SI sont les plus susceptibles d'être ciblés par ce type de malware vu qu'ils sont responsables de tout type de données (même les plus sensibles).

> Les entreprises et les organismes publics

Soucieuses de la confidentialité de leurs données, les entreprises telles que les institutions financières sont les cibles de choix des pirates. De plus, tout organisme à caractère public ayant accès à des données sensibles et confidentielles peut être une cible idéale pour les ransomwares.

Moyens d'infection

Internet et réseaux sociaux

C'est le mode de transmission principal de ce type de malware et ce via des pièces jointes contaminées ou des liens douteux (sur facebook par exemple).

Réseaux d'entreprise

Il suffit d'infecter une seule machine faisant partie d'un réseau pour que le ransomware exploite les failles de sécurité de ce réseau (LAN, MAN) pour s'y propager.

Disques amovibles

Comme tout malware, le ransomware peut infecter des supports de stockage amovibles et infecter davantage de machines.

Comment se protéger des Ransomwares ?

Prévenir c'est sécuriser !

Auditez votre système d'information d'une manière périodique afin de détecter les eventuelles failles relatives aux differentes composantes de votre système d'information. La mise en place d'une politique de sécurité vous permettra d'optimiser la sécurité du périmètre de votre système d'information.

Opter pour une infrastructure logicielle fiable !

Comme tous les malwares, les ransomwares exploitent les failles logicielles des différentes composantes de votre architecture logicielle. De ce fait, il est primordial de mettre à jour les élèments vitaux de votre système d'information tels que les systèmes d'exploitation et les solutions de protection (Antivirus, Firewalls, IDS/IPS).

Sensibiliser les employés !

Un malware peut être transmis de plusieurs manières et dans la plupart des cas, suite à des failles humaines induites par un manque de connaissance. Il est donc, crucial d'organiser des sessions de sensibilisation aux cyber attaques à tous les employés y compris les administrateurs du SI.

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

tunCERT
Tunisian Computer Emergency ResponseTeam