LES NOUVEAUX VIRUS RANSOMWARE

Le début d'année 2016 est un challenge en matière de sécurité des SI pour les entreprises. En effet, les nouveaux logiciels malveillants appelés "Ransomware" prennent pour cible aussi bien les grandes entreprises privées ou les institutions publiques que les PME en prenant en otage leur système d'information et les données de leurs collaborateurs.
Edgar Kouliche, Président et Directeur Technique de Quantic nous explique comment se comporter face à ces Ransomwares.

«*Les RansomWares sont des logiciels malveillants qui cryptent vos données. Le principe est celui d'une prise d'otage. Ils kidnappent vos informations en demandant une rançon en échange de leur libération. Ces Ransomwares se cachent dans les pièces jointes de mail sous forme, par exemple, de factures d'opérateurs téléphoniques dont la ressemblance avec les vraies est suffisante pour que l'utilisateur peu attentif se fasse piéger. C'est pourquoi il est indispensable de vérifier l'authenticité du mail et ne jamais ouvrir de pièces jointes quand l'émetteur du mail (adresse de l'émetteur et pas seulement le nom affiché) est inconnu.*»

Dès lors que le malware a réussi à s'implanter et que les premiers effets apparaissent, on peut envisager deux types de réaction semblables à celles des Etats dont les citoyens sont pris en otage.

- Vous avez le choix de payer le rançonneur afin qu'il vous envoie, en échange, la clé permettant de décrypter vos données. Cette solution revient à faire confiance à votre agresseur pour qu'il vous rende l'accès à votre bien après votre paiement. C'est aussi l'encourager à recommencer. Cependant, en fonction de votre capacité à remettre vous-même votre SI en état, elle est parfois la seule issue et l'agresseur compte là-dessus.
- Vous pouvez également procéder vous-même au déverminage des postes et serveurs infectés par le malware à condition de vous être mis en situation de répondre à ce type d'agression avant qu'elle ne survienne. Il faut alors être en mesure :
    - d'arrêter la propagation avant que la situation ne devienne incontrôlable ;
    - de déverminer les postes et serveurs non sauvegardés ;
    - de restaurer une sauvegarde récente et SAINE (la vérification des contenus est obligatoire) de vos données.

Quelle que soit la solution choisie, vous devrez **réviser et réévaluer vos politiques de sécurité** et leur implémentation afin d'augmenter le niveau de sécurité de votre SI.

Edgar KOULICHE

Président & Directeur Technique de Quantic

Information

Quantic
5 avenue de Verdun
94200 Ivry-sur-Seine

Tel : 01 85 33 01 30
Mail : contact@quantic.fr

Best Practices :

1. Mise en place d'une Sauvegarde efficace et régulière (Ex : Backup Exec)
2. Amélioration de la Gestion des accès des collaborateurs aux ressources (droits sur les fichiers / GPO / Administration des serveurs et postes / …)
3. Mise en place d'outils tels que des : anti-virus (Ex : Symantec Endpoint Protection) / anti-malware / Anti-spams (Ex: Symantec Messaging Gateway) / ATP
4. Mise en place d'outils détecteurs d'attaques (Ex : SIEM)

Pour découvrir ces solutions de sécurité, cliquez sur le lien suivant : http://bit.ly/22lWaQV

Mais selon Edgar Kouliche, le plus important reste à faire :
« *Malgré l'implémentation de toutes ces mesures sécuritaires, tout repose sur* ***la vigilance de chaque utilisateur*** *qui DOIT être sensibilisé à ces problématiques de sécurité au sein de son entreprise et averti des risques et des moyens de s'en prémunir.* »