Traiter les courriers électroniques malveillants [1]

Régulièrement les boîtes aux lettres électroniques de l'Etat reçoivent des courriels malveillants qui contiennent des fichiers espions.

Récemment, la direction générale des systèmes d'information (DGSI) a repéré des courriels provenant d'une attaque à large échelle puisqu'elle a touché nombreuses administrations fédérales, cantonales et communales. Il s'agit d'applications qui, une fois exécutées, scannent tous les disques réseaux auxquels l'ordinateur a accès, avec ou sans droits d'administration. Ils les rendent inutilisables pour quiconque. Enfin, ils utilisent également les adresses contenues dans l'ordinateur pour se propager. En clair, tout ordinateur ou disque réseau infecté doit être reconfiguré.

Heureusement, ces courriels malveillants **sont faciles à reconnaître** (comme le montre l'illustration ci-dessus), car ils possèdent des caractéristiques communes :

- Ils sont envoyés depuis un expéditeur, **dont l'identité est souvent – mais pas toujours – connue** du destinataire.
- Ils possèdent **des adresses électroniques étranges et peu communes** : @trademarket.com, @gulash.net etc.
- Ils ne contiennent **pas de sujet**.
- Ils contiennent en pièce jointe **un fichier de type « .zip »**. C'est ce fichier qui contient l'application espionne.

La **solution** pour éviter d'être atteint par ce virus et d'en stopper la propagation est finalement **aussi simple que capitale** :

1. Il importe avant tout **de ne pas ouvrir le message reçu**, même s'il provient d'un expéditeur connu.
2. Quand bien même le message aurait été ouvert par inadvertance, il importe **alors de ne pas ouvrir la pièce jointe** possédant l'extension « .zip ».
3. Si malgré tout, le fichier « .zip » devait être ouvert et les fichiers qu'il contient devaient être visibles, **il ne faut surtout pas les ouvrir**.

De son côté, la DGSI prend toutes les mesures nécessaires pour empêcher la propagation de ces applications néfastes.

Rappelons que **le comportement adéquat** des titulaires de comptes de messagerie de l'Etat constitue la meilleure des parades. Ainsi, il est important de répéter que tout message qui paraît suspect ne doit jamais être ouvert et encore moins les pièces jointes qu'il pourrait contenir.

SEM Logistique

Bernard Magnenat

Rue des Gazomètres 3
Case postale 241
1211 Genève 8

URL source (modified on 07/12/2015 - 11:55): https://edu.ge.ch/sem/usages/outils/traiter-les-courriers-electroniques-malveillants-1405

Liens
[1] https://edu.ge.ch/sem/usages/outils/traiter-les-courriers-electroniques-malveillants-1405