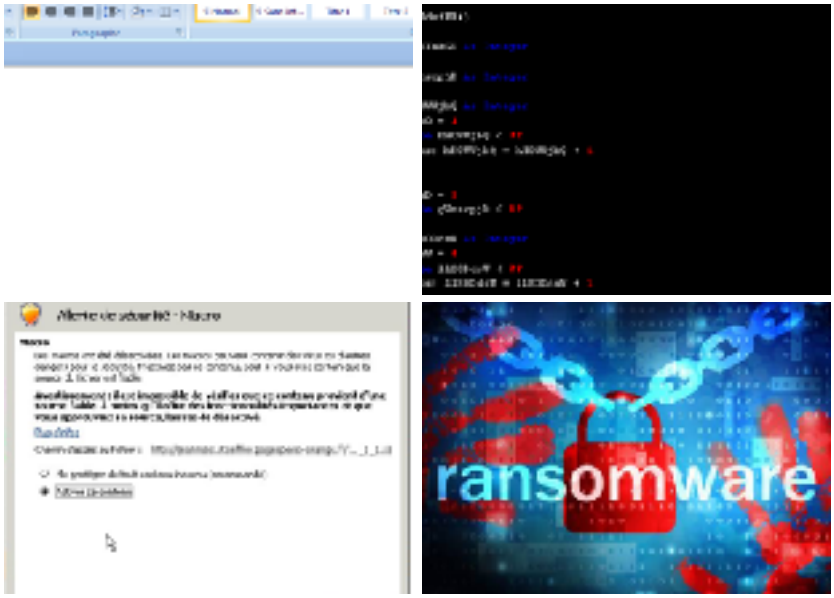
R.S.S.I.
Laurent Péquin
Université de La Réunion
14 octobre 2016

Vague de spams sur fond de fausses factures

Le contenu du mail est toujours très succinct, le document « semble » vide, et une Macro tente de s'exécuter (refusez l'exécution)



Le fonctionnement

Le mail reçu se présente de façon anodine : la plupart du temps, une relance de facture, incluant une pièce jointe au format **.doc** ou **.xls** de Microsoft Office. À l'heure actuelle, peu d'antivirus détectent la nouvelle variante de ce logiciel (qui est signé avec un certificat officiel paraissant émaner de l'entreprise de sécurité Comodo), et la plupart ne suppriment donc pas la pièce jointe.

Si le destinataire tente d'ouvrir le document Word joint, une page vierge va s'afficher, mais le logiciel de Microsoft va tout de même demander à l'utilisateur s'il veut activer les macros (permettant d'interpréter les codes éventuellement contenus dans les documents Office). Une réponse positive active le virus et va lancer le téléchargement discret d'un premier code malicieux.

D'autres fichiers sont ensuite téléchargés afin d'installer divers programmes-espions. Il ne reste plus au pirate qu'à décider quand et quel programme utiliser et installer pour récupérer les données personnelles et bancaires puis effectuer des opérations frauduleuses.

A quoi ressemblent ces courriels piégés ?

Les premières vagues de mails, le plus souvent intitulés « *Relance Facture urgent* » ou de « *AR CDE + Facture Proforma* », ont touché des messageries personnelles ou d'entreprises dès le mois de juin. Ecrits dans un français très correct et sans fautes d'orthographe, ces textes courts, et suffisamment sibyllins pour inquiéter ceux qui les reçoivent, ont déjà fait l'objet d'une première alerte officielle émanant du CERT-FR, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques. La nouvelle vague de mails reçus ces deux dernières semaines sont du même tonneau. Exemples :

« Objet : PIXOLUTIONS - FACTURE N°03480830-260615
Bonsoir,
Veuillez trouver en pièce jointe la facture n°03480830-260615 correspondant à la réalisation et pose du logo végétalisé à Perpignan.
Vous en souhaitant bonne réception, bien cordialement, ».

« Objet : DUPLICATA FAC N°87878241
Salut,
Il parait que tu recherches la facture avec les Rimauresq Rosé et Blanc ?
La voici en pièce jointe. Veux-tu que je te la remette au courrier également ? »

« Objet : Comptabilité de PACAR : facture n° 94352132 du 26/10 de 439,99 euros
Bonjour,
Pouvez-vous nous envoyer un chèque de 439,99 euros en paiement de la facture n° 94352132 dont vous trouverez la copie ci-jointe. En vous remerciant, Bien cordialement, »

Comment s'en protéger ?

En plus d'un antivirus à jour (vous pouvez demander à votre informaticien de proximité préféré), il est recommandé d'observer une grande vigilance à la réception de tout message contenant une pièce jointe, **et ce quel que soit son format** (.doc, .odt, .xls, .pdf, etc.).

Si le courriel semble émaner d'un organisme officiel (administrations, banques, boutiques en ligne, etc.), il est préférable de tenter de les contacter soit par téléphone, soit par mail pour vérifier l'objet de la correspondance et la légitimité de l'envoi (un peu lourd parfois, mais ô combien nécessaire).

Enfin, l'étape de sécurité optimale consiste à désactiver l'exécution automatique des macros dans les suites bureautiques de type Microsoft Office (aller dans Fichiers/Options/Centre de gestion de la confidentialité/Paramètre du Centre de gestion de la confidentialité/Paramètres des macros/Désactiver toutes les macros avec notifications).

Comment vérifier sa présence et s'en débarrasser ?

En cas de doute, contactez immédiatement votre informaticien de proximité, et/ou faites une demande de travaux : https://dt.univ-reunion.fr/