SOLUTIONS INFORMATIQUES

Distributeur :

PARC CERES – 21 rue Ferdinand BUISSON – Bât. O 53810 CHANGE
Tél : 02 43 69 72 37 – Fax : 02 43 68 62 15 – Email : info@solutions-informatiques.fr

Nouvelle vague de « Ransomwares »

Depuis quelques jours nous assistons à une nouvelle attaque virale de type « cryptolocker » ou « ransomware ».

Ces virus sont diffusés par mail, dans des pièces jointes essentiellement de type Office avec macro.

Nous vous conseillons donc de faire très attention aux messages que vous recevez actuellement.

Ces virus cryptent vos données et se diffusent via le réseau en empruntant toutes les chemins non sécurisés. Le but des pirates étant de vous faire payer des clés de décryptage sur le Dark Web à partir d'environ 300 €.

COMMENT FONCTIONNE LE VIRUS :

Vous recevez un spam avec une pièce jointe de type .doc ou .xls. Ce document, une fois ouvert est illisible, et vous demande d'autoriser les macros. Il peut également s'installer depuis une pages internet.

En acceptant les macros, vous enregistrez un fichier qui sera exécuté plus tard. L'exécution de ce fichier télécharge un outil de cryptage de vos données.

Une fois vos données cryptées, vous aurez un avertissement sous forme de fenêtre ou par changement de votre fond d'écran.

Le Ransomware s'attaque à tous types de systèmes, aussi bien Windows que Linux ou encore Mac OS. Il est aujourd'hui indétectable par les anti-virus classiques.

Précautions à prendre

- Ne cliquer que sur les pièces jointes et liens de téléchargements de destinataires identifiés.
- Réaliser une sauvegarde systématique des données (idéalement multiple et multi sites) et déconnectez vos supports de vos ordinateurs et serveurs.
- Avoir un antivirus professionnel
- Utiliser un antivirus à jour
- D'une façon générale, les opérateurs institutionnels n'envoient aucune pièce jointe (factures, notices, documentations, …)

SOLUTIONS INFORMATIQUES

Distributeur : sage ebp codial centre intégrateur

PARC CERES – 21 rue Ferdinand BUISSON – Bât. O 53810 CHANGE
Tél : 02 43 69 72 37 – Fax : 02 43 68 62 15 – Email : info@solutions-informatiques.fr

Les stratégies sont nombreuses pour vous faire cliquer sur un lien ou un fichier viral :

- Factures téléphoniques, EDF, documents bancaires
- Factures de prestataires ou fournisseurs
- CV de candidats, notes de services
- Ces documents peuvent être des pièces jointes (pdf, zip, rar ou tout fichier bureautique) ou des liens vers internet (sites web, liens DropBox, …)
  En cliquant sur ces liens ou en suivant ces liens, le virus est déclenché, la propagation et inéluctable.

L'objectif est de créer la confiance ou le doute pour vous faire cliquer le plus rapidement possible.

Les éléments à vérifier si vous avez des doutes sur un mail :

Faites preuve de jugement quant aux messages (e-mails, tweets, messages Facebook,) que vous recevez. Sachez reconnaître les signes douteux :

- Messages ne contenant qu'un lien ou dans une langue étrangère à l'expéditeur,
- Adresse courriel de l'expéditeur différent du vrai domaine de l'entreprise.
  (ex :e.gdesjardins.com : moneybank@sgdesjardins.com ou desjardins@caisses.com)
- URL de destination différente de celle affichée dans le message (en survolant l'URL affichée vous pouvez voir l'adresse vers où vous serez redirigé).
- Ne naviguez pas sur des sites à apparence louche. Souvent les navigateurs peuvent reconnaître si des scripts menaçants tournent sur ces sites et vous en aviseront, n'ignorez alors pas ces avertissements de sécurité !

Le plus important : faites des sauvegardes régulières de vos données (dossiers, courriels, …) sur supports dématérialisés, sur NAS ou disque externe en les déconnectant après la réalisation de la sauvegarde et surtout, **Vérifiez** que votre sauvegarde est valide : En effet les sauvegardes sont inutiles si vous ne pouvez pas les utiliser pour effectuer une restauration. La restauration d'une sauvegarde viable est le seul moyen de retrouver vos données après une infection de votre système d'information.

Un doute sur l'état de votre protection ?

Notre équipe reste à votre disposition pour plus d'informations sur les risques de ce virus et les produits qui peuvent permettre de le contrôler.

SOLUTIONS INFORMATIQUES

02 43 69 72 37
info@solutions-informatiques.fr
www.solutions-informatiques.fr

LES SOLUTIONS

La sauvegarde en ligne

Pour vous prémunir des risques occasionnés par une éventuelle infection d'un cryptovirus, il existe la solution SIBACKUP basée sur un logiciel qui permet ensuite de créer, programmer et lancer une sauvegarde des données de vos fichiers vers un espace de stockage sécurisé et hébergé chez des prestataires spécialisés.

Avec SIBACKUP vos données sauvegardées sont récupérables en temps réel pour reprendre très rapidement votre activité.

Avec SIBACKUP, le cryptage de vos données en 256bits, la compression de vos fichiers et la sécurisation des connexions entre vos fichiers et les serveurs vous offrent une solution de télé-sauvegarde sûre et efficace.

La sauvegarde sur supports physique

SPX

STORAGECRAFT SHADOWPROTECT

StorageCraft Recovery Solution forme la base de la continuité d'activité. Protégez les systèmes, les données et votre tranquillité d'esprit à l'aide de sauvegardes vérifiées et d'options de reprise rapide. Que vous utilisiez un environnement Windows ou Linux, physique ou virtuel, nous avons ce qu'il vous faut.

mailinblack email to network

MailInBlack, la solution 100 % efficace face aux cyber-attaques !

eset SMART SECURITY

Augmentez les règles de sécurité de votre antivirus : Grâce à **ESET PROTECTION ADVANCED**, vous pouvez consulter vos comptes bancaires, surfer sur les sites d'achats en ligne et effectuer vos transactions de manière plus sécurisée. Comptez sur une **suite de sécurité Internet complète** qui intègre un antivirus, un pare-feu personnel et bien plus de fonctionnalités.

Enfin communiquez avec vos collaborateurs sur les risques liés aux ransomwares dans les emails car le meilleur moyen de ne pas être infecté est de ne pas les ouvrir.