Actualité

Alerte sécurité entreprise – Curriculum Vitae avec ransomware GoldenEye - 20/01/17

Des cybercriminels se présentent comme des demandeurs d'emploi dans le cadre d'une nouvelle campagne visant à infecter les départements ressources humaines des entreprises.

Les départements ressources humaines doivent donc se méfier de certains candidats prétendus dont l'objectif est de les infecter avec le ransomware GoldenEye et exiger ensuite le paiement d'une rançon.

Cette variante du ransomware Petya ne vise pas les RH par hasard. Ceux-ci sont en effet souvent amenés à ouvrir les pièces jointes de contacts inconnus dans le cadre de leur mission de gestion des recrutements.

Un premier fichier PDF inoffensif concernant une demande d'emploi est généralement envoyé pour endormir la méfiance. Le virus est adressé lors de l'envoi d'un second fichier infecté, pouvant être un curriculum vitae.

Préconisations :
- "On réfléchit puis on clique et non pas l'inverse". Seule une vigilance permanente permet d'éviter les désagréments causés par un ransomware.
- Réalisez des sauvegardes très régulières et en vérifier la viabilité. En cas de problème, cette action est la seule permettant un retour à la normale (plus ou moins rapide) après avoir subi ce type d'atteinte.
- Mettre en place une veille "cyber" pour se tenir au fait de toute nouvelle évolution des risques.
- Consultez le site de l'agence nationale de sécurité des systèmes d'information (ANSSI) **www.ssi.gouv.fr.**
- Informez votre hiérarchie ;
- Déposez plainte si vous le souhaitez auprès des services de police ou de gendarmerie ou faite une déclaration directement sur le site de pré-plainte en ligne **https://www.pre-plainte-en-ligne.gouv.fr** ;
- Restez vigilant.

Source : Adjudant-chef ROUBEY, rédacteur de la note
intel-eco.rgfc@gendarmerie.interieur.gouv.fr