



## Mesures préventives contre « WannCry »

Récemment, une campagne massive de Spam, portant comme pièce jointe un nouveau ransomware baptisé « WannaCry », a été détectée sur le net. Connue aussi sous les noms Wana Decrypt0r, ce malware est capable d'exploiter la faille « MS17-10 » du composant « Microsoft Server Message Block SMBv1 » pour obtenir des privilèges élevés, crypter les données personnelles des victimes et aussi se propager sur d'autres machines vulnérables. Pour s'en protéger, nous vous conseillons d'être vigilant et de suivre les mesures préventives suivantes :

- Vérifier l'authenticité et la fiabilité des expéditeurs avant la lecture de chaque message reçu par e-mail ou affiché sur votre mur de Facebook / Twitter et en cas de doute n'y répondez pas, ne cliquez pas sur les liens hypertextes ou les images qu'il contient et supprimer le immédiatement.
- Mettre à jour régulièrement votre solution antivirus.
- Activer la mise à jour automatique de votre système Windows.
- Sauvegarder régulièrement vos données sensibles sur des disques durs externes.
- Créer chaque semaine des points de restauration pour récupérer les fichiers système en cas d'infection.
- Installer des Addons dans votre navigateur web pour vous renseigner sur la fiabilité des sites web visités (Exemples: Netcraft ).
- Utiliser un compte utilisateur avec des privilèges limités pour se connecter à Internet.