La diffusion planétaire d'un rançongiciel a été détectée en France vendredi 12 mai.

Un cocktail détonant a semé la panique en Espagne, puis dans le monde entier. En quelques heures, le rançongiciel WannaCry s'est taillé un succès planétaire, multipliant les infections dans plus de 70 pays. Parmi ses victimes, l'opérateur Telefonica, les banques BBVA et Santander, le fournisseur d'électricité Iberdrola, le logisticien Fedex, la compagnie ferroviaire allemande Deutsche Bahn ainsi que l'opérateur de télécommunications Vodafone, mais aussi, en France, Renault, le système de santé britannique le NHS, …

Renault a admis avoir été pris dans la nasse de WannaCry, entraînant la mise à l'arrêt de certains sites de production afin « *d'éviter la propagation du virus* ». De source syndicale, l'usine de Sandouville (Seine-Maritime), qui emploie 3400 salariés, serait ainsi concernée, tout comme le site d'une filiale du groupe en Slovénie, à Novo Mesto.

L'Agence Nationale pour la Sécurité des Systèmes d'Information ANSSI explique qu'aucune autre infection majeure ne serait à déplorer dans l'Hexagone.

En somme, une cyberattaque d'un « *niveau sans précédent* » selon Europol. Dans la nuit de vendredi à samedi, un ingénieur de l'éditeur d'antivirus Avast, Jakub Kroustek, dénombrait plus de 100 000 systèmes Windows infectés en moins de 24 heures, **57 % d'entre eux étant situés en Russie.**

Devant l'urgence de la situation, Microsoft a d'ailleurs sorti des **correctifs** pour ce type de failles sur Windows XP, Windows Server 2003 et Windows 8.

http://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel-2/

Conseils pratiques

La prévention est essentielle :

- Etre à jour en permanence avec les logiciels et dispositifs de sécurité (antivirus, Operating système, firewall, …)
- Entraîner la chaîne d'alerte et les acteurs opérationnels et décisionnels
- Sensibiliser les utilisateurs à ne pas ouvrir des mails douteux.

En termes de protection il est nécessaire

- D'avoir des sauvegardes complètes contrôlées régulièrement
- De mettre en place des Plans de Continuité d'Activité Cyber prévoyant la remontée d'alerte, la communication et le fonctionnement de l'entreprise pendant cette période instable
- De tester régulièrement ces Plans