Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

Service spécialisé de défense et de sécurité

Le haut fonctionnaire de défense et de sécurité

HFDS
N°2017 - 633

Affaire suivie par :
Benoît MOREAU
Fonctionnaire de sécurité des systèmes d'information

Téléphone
01 55 55 84 85

Mél.
benoit.moreau@education.gouv.fr
benoit.moreau@recherche.gouv.fr

99, rue de Grenelle
75357 Paris 07 SP

Paris, le 15 MAI 2017

Le haut fonctionnaire de défense et de sécurité

à

Mesdames et messieurs les recteurs d'académie

Mesdames et messieurs les présidents et directeurs généraux des établissements de l'enseignement supérieur

Mesdames et messieurs les présidents et directeurs généraux des organismes de recherche

Mesdames et messieurs les directeurs généraux et directeurs des établissements publics du scolaire.

Objet : Prise en compte de la cyber attaque mondiale « WannaCry »

Référence : Bulletin d'alerte ANSSI du 14 mai 2017.

Depuis le 12 mai 2017 une cyber attaque majeure est en cours et est largement relayée dans les médias. Le virus chiffre les données et demande une rançon de quelques centaines d'euros pour rendre l'accès aux informations. La criticité de la situation est liée à sa capacité à se propager entre les ordinateurs au sein du réseau des entités. Une personne infectée via un mail malveillant ou une navigation sur un site compromis peut ainsi exposer l'ensemble des ordinateurs de ses collaborateurs.

Pour l'instant les établissements du ministère ne semblent pas être massivement touchés. Le redémarrage des postes de travail accompagnant la reprise de la semaine risque cependant de favoriser la propagation du virus.

Afin de limiter les infections et la propagation, Microsoft a publié un correctif et des mesures de cloisonnement peuvent être mises en place. Les mesures préventives indispensables restent la sauvegarde régulière et la sensibilisation des personnels. Les responsables de la sécurité des systèmes d'information (RSSI) ainsi que les directeurs des systèmes d'information académiques ont d'ores et déjà été alertés.

L'ANSSI recommande de ne pas payer la rançon qui ne garantit pas la récupération des données. De plus cela favorise le développement de ces attaques et risque de compromettre les moyens de paiement.

Cette crise cyber nécessite une extrême vigilance et l'implication de chacun, une première fiche de posture est jointe à cette note. Les nouvelles informations qui pourraient apparaitre seront diffusées via les chaines opérationnelles par mes équipes qui restent à votre disposition.

Le haut fonctionnaire de défense et de sécurité

Frédéric GUIN

PJ : fiche « posture MENESR face à l'attaque WannaCry »