Posture MENESR face à l'attaque « WannaCry »

Nous connaissons un épisode sans précédent en terme de gravité de diffusion d'un virus/ver de crypto virus dont le nom de code est notamment « WanaCrypt0r » (cf. alerte CERTFR-2017-ALE-010[i]). Cette attaque largement médiatisée utilise pour se répandre la faille Microsoft sur TCP/445 - SMBv1 décrite dans le bulletin MS17-010[ii]

La propagation de la première version de ce rançongiciel semble avoir été stoppée suite à l'activation d'un « kill switch » par un chercheur anglais en cybersécurité. Selon les informations émanant de l'ANSSI, une nouvelle version sans ce « kill switch » circulerait déjà.

Il est demandé de prendre les mesures suivantes sans attendre :

Mettre à jour

- Mise à jour de tous les périmètres suivant les indications déjà reçues des CERT ou de Microsoft : serveurs, postes de travail. Si les systèmes utilisés ne sont plus aptes à recevoir une MAJ Microsoft, conformément à la PSSIE il doit être confiné dans un réseau isolé
- Mettre à jour régulièrement les bases de signatures des antivirus et des différents équipements de sécurité pour prendre en compte toutes les nouvelles variantes qui pourraient apparaitre.

Sauvegarder

- Assurez-vous d'avoir des sauvegardes effectives et hors lignes des données.
- Envisagez l'augmentation de leur fréquence.

Informer

Informer tous les agents de votre périmètre et des périmètres adjacents [Acteurs : DSI, RSSI, service Communication], par exemple :

- Rappelez les consignes d'usage de la messagerie, en particulier de la vigilance accrue sur l'ouverture de pièces jointes ou les liens suspects, par exemple sur la première page de tous vos intranets.
- Demandez aux équipes bureautiques de fournir des accompagnements personnalisés.
- Faire savoir que toutes les données sensibles qui ne le seraient pas doivent être sauvegardées en réseau.

Cloisonner

- Envisager autant que faire se peut de cloisonner les ports SMB/CIFS - filtrage en périphérie du réseau.
- Selon situation locale, envisager des mesures de cloisonnement à prendre en lien avec les autorités académiques.

Désactiver les services inutiles

- Désactiver si possible le support du protocole SMBv1 (si tous les clients de votre réseau peuvent utiliser SMBv2 ou v3)

https://support.microsoft.com/fr-fr/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012

Surveiller

- Mesures du taux de postes potentiellement infectés (v1 du rançongiciel) par recensement de l'activité sur l'URL http : hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com *(URL modifiée dans ce message pour la rendre non cliquable, remplacer hxxp par http et enlever les crochets afin de la rechercher dans les journaux des proxys par exemple)*

En cas d'infection avérée

- Déconnectez immédiatement le poste infecté du réseau.
- Ne pas payer la rançon.
- Alertez immédiatement les correspondants SSI/DSI.
- remonter spécifiquement les incidents majeurs et statistiques à :

incident-ssi@education.gouv.fr

Nous restons mobilisés sur le sujet et attendons un acquittement de votre part par retour de mail sur la bonne prise en compte de ce message de mobilisation.

---

[i] https://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel-2/
[ii] https://technet.microsoft.com/fr-fr/library/security/ms17-010.aspx