POLICE NATIONALE

DIVISION DE L'ANTICIPATION ET DE L'ANALYSE

ALERTE

13 mai 2017

Direction Centrale de Police Judiciaire
Sous-Direction de la lutte contre la cybercriminalité

WCRY

Les établissements hospitaliers britanniques sont actuellement ciblés par une campagne d'attaques par rançongiciels ou ransomwares baptisée WCry qui entrave voire empêche leur activité. Elle concerne les ordinateurs fonctionnant sous Windows (toutes versions confondues).

Le phénomène a déjà touché le territoire français.

La nouveauté réside dans le mode de propagation du logiciel malveillant. Les rançongiciels traditionnels n'affectent qu'une seule machine à la fois : ils sont transmis par mail, site infecté ou autre logiciel malveillant, bloquent le poste infecté en chiffrant les fichiers et affichent le message de rançon. WCry se transmet à toute autre machine connectée et se répand, provoquant une épidémie.

Pour s'en protéger, les ordinateurs doivent avoir installé le correctif Windows MS17-010.
https://technet.microsoft.com/fr-fr/library/security/ms17-010.aspx

La SDLC a ouvert une enquête en flagrance et est le point de contact national avec Europol.

1. Origine

Fin 2016, des outils d'intrusion informatique développés par la NSA ont été diffusés sur Internet par un groupe inconnu du nom de Shadowbrokers. Ceux-ci souhaitaient tout d'abord vendre ce matériel de guerre numérique au plus offrant mais, faute d'acheteur, l'ont diffusé largement à titre gracieux.

Parmi ces outils offensifs se trouvait un rançongiciel d'un genre nouveau, WCry.

2. Conduite à tenir

Le ransomware se propagerait par les ports 138, 139 et 445, utilisés par les protocoles SMB et MBT.
L'infection initiale n'est pas connue avec certitude : hameçonnage, site web infecté ou téléchargement par un autre logiciel malveillant. L'infection exploite ensuite la faille corrigée dans le bulletin MS 17-010 de Microsoft.

La propagation de l'infection serait terminée, enrayée suite à l'intervention du chercheur en cybersécurité Malwaretech :
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

Toutefois, afin de se protéger efficacement en cas de résurgence du logiciel malveillant, il est recommandé de :

- En cas de poste infecté : débrancher et isoler voire éteindre toute machine infectée pour limiter la propagation de l'épidémie

- Contrôler que tous les postes Windows, quelle que soit la version, aient fait l'objet du correctif MS 17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx)

- Mettre sous surveillance le trafic réseau, notamment les ports 138, 139, 445 qui seraient les vecteurs de propagation du logiciel malveillant

- Ne pas bloquer les communications vers le domaine suivant : iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

- En cas d'infection, prendre contact avec le CSIRT-PJ à l'adresse :

csirt-pj@interieur.gouv.fr