Active Circle

Technical Brief

Se protéger des attaques de ransomwares Active Circle

Mai 2017

oodrive
Trusted Cloud Solutions

Se protéger des attaques de ransomwares

1. Désactiver le serveur SMB (CIFS) sur chacun des nodes Active Circle sur lesquels il est activé. Tous les partages deviennent alors inaccessibles en SMB/CIFS, mais restent accessibles en FTP et/ou NFS.

2. Valider que l'intégralité des clients SMB/CIFS du parc de machines est correctement protégé, et que les machines infectées ont été totalement isolées,

3. Etape optionnelle et temporaire, mais recommandée afin de parer à une future propagation, dans la console d'Administration d'Active Circle :
    - Activer l'historisation sur les partages sur lesquels elle ne l'était pas,
    - Activer également la rétention des fichiers supprimés sur toutes les stratégies d'historisation sur lesquels elle ne l'était pas
    - Désactiver temporairement la programmation de la stratégie d'historisation sur chacun des partages sur lesquels elle était activée.

4. Réactiver le serveur CIFS sur chacun des nodes sur lesquels il a été désactivé à l'étape 1.

Une fois que les risques liés à WannaCry auront fortement diminué, les actions effectuées à l'étape 3, pourront être annulées. Il sera notamment important de reprogrammer la stratégie d'historisation pour éviter que les versions de fichiers ne s'accumulent et ne remplissent l'espace de stockage.

Si toutefois la propagation avait déjà eu lieu : si la fonctionnalité d'historisation d'Active Circle avait été activée sur les partages impactés, alors il sera possible de récupérer la version originale des fichiers, voire même les fichiers supprimés.

Cette Procédure est valable pour toutes les attaques de même type.