Forum: Dépannage

Topic: Points de restauration intempestifs

Subject: Re: Points de restauration intempestifs

Publié par: JF-33

Contribution le : 31/08/2018 20:16:46

Citation :

alain70 a écrit:
Le problème semble résolu les points de restaurations crees par Defender juste avant la maintenance automatique ont disparus .
Defender fonctionne normalement , mise à jour et protection . L'analyse du système se fait automatiquement comme avant .
Je pense que vous avez bien mis le doigt sur ce fameux bug .
Reste à avoir l'avis d'autres personnes .
Merci Cordialement.

Bonjour Alain, merci de cette confirmation que Windows Defender fonctionne malgré la désactivation de la tâche planifiée "Windows Defender Verification". J'espère qu'il n'y aura pas d'effets inattendus, prend bien note de cette modif. J'ai simplement rapporté que cette tâche avait un rôle à jouer dans ce nouveau comportement de Windows ; le bug reste à identifier.

Résumé des observations:
Rappel: le *mardi* 31/07/2018 une mise à jour a eu lieu ; les PR "Programme d'installation pour les modules Windows" sont apparus le lendemain 1er août.

On a vu que désactiver la Tâche Planifiée "Windows Defender Verification" stoppe le phénomène.
Activer à nouveau la Tâche ==> les PR reviennent.

L'examen de cette tâche révèle que l'exécutable utilisé est justement daté du 31/07/2018:
Extrait du XML de la tâche:
Tâche de vérification périodique : Windows Defender Verification
Aucun déclencheur
LocalSystem S-1-5-18
Privilèges : HighestAvailable
AllowStartOnDemand : true
Commande :
C:ProgramDataMicrosoftWindows Defenderplatform4.18.1807.18075-0MpCmdRun.exe
Arguments : -IdleTask -TaskName WdVerification

Appellation interne de MpCmdRun.exe =
Microsoft Malware Protection Command Line Utility
Version : 4.18.1807.18075
Modifié le : 31/07/2018 12:17 <== le 31/07 !
Il y a un log, accessible en tant qu'admin :
C:WindowsTempMpCmdRun.log

Lancer manuellement la tâche "Windows Defender Verification" ne crée pas de PR
Heureusement provoquer une Maintenance crée à chaque fois un PR (seulement si la tâche est activée, off course).

La commande pour lancer une Maintenance doit être accompagnée de l'argument start:
MSCHEDEXE.exe start
Le nom interne de cette commande est "Maintenance automatique".
L'argument *start* est obligatoire, sinon il semble ne rien se passer ; la commande n'est pas bavarde, et il n'y a pas d'aide.
C'est très pratique pour faire des tests.
Avant de lancer la commande, préparer le gestionnaire des tâches. Après un moment, l'activité devient intense, surtout disque.
Dans les processus on repère defrag, cleanmgr, TrustedInstaller, et TiWorker qui prend parfois 50% d'activité, voir plus bas.

EVERYTHING est le gratuiciel que j'utilise le plus. Il sert normalement pour trouver en un temps record des fichiers. Mais si on classe TOUS les fichiers par ordre de date de modification, ou de création, c'est intéressant d'observer ce qui se passe pendant la Maintenance.
Un PR ayant été créé, je note l'heure de sa création : 12:12
Dans les fichiers CRÉÉS à 12:11 il y a des XML stockés en c:WindowsservicingSessions
Exemple:
C:WindowsservicingSessions30687567_3649252512.xml

Au sujet des réglages pouvant influencer la création des PR, je n'ai pas obtenu de résultat ; bloquer la stratégie "Créer un point de restauration système" est ignorée, c'est surprenant.

Côté registre :
HKLMSOFTWAREMicrosoftWindows NTCurrentVersionSystemRestore
RestoreStatusDescription = Programme d’installation pour les modules Windows
Voilà la raison du nom de ces points.
SystemRestorePointCreationFrequency = 0
RPGlobalInterval = 1
C'est une valeur qu'on pouvait faire varier de 86400 secondes par défaut (24h) à beaucoup plus pour espacer les points ; plus aucun effet. Au contraire le système me l'a repositionné d'autorité à 1.

Côté Services on a :
- "Programme d’installation pour les modules Windows"
  TrustedInstaller Manuel
- "Sauvegarde Windows"
  SDRSVC Manuel

Un programme est souvent évoqué sur le net comme responsable de gels. Il est effectivement très actif pendant les Maintenances:
TiWorker.exe = Windows Modules Installer Worker

Mon eeePC sorti du placard s'est enfin mis à faire ces PR comme tout le monde.

Un autre fil de discussion pour finir:
TROP DE POINTS DE RESTAURATION 18/08/2018

http://dechily.org/Forum_Aski/viewtopic.php?f=63&t=2134
Gratilog est cité, ce sont des habitués. Restore Point Creator est vu (un moment) comme cause possible du phénomène ; il n'en est rien, ces PR sont aussi présents chez les utilisateurs standards. Ce sympathique RPC, comme il a été dit, ne sera plus mis à jour. Tom abandonne son développement et encourage à sauvegarder des images du disque système.

CONCLUSION
Le phénomène est apparu avec MpCmdRun version du 31/07/2018.
Un contournement consiste à désactiver la Tâche Planifiée "Windows Defender Verification". RPC est capable au besoin de créer des PR automatiquement. Il existe également un script VBS à installer comme Tâche Planifiée.
Installer un autre antivirus met normalement au silence Windows Defender. Je ne sais pas ce qui se passerait pour la Tâche Planifiée "Windows Defender Verification" ; vu son utilisation par la Maintenance, il est à supposer qu'elle resterait active.

À suivre !