Connaissez-vous les fichiers Prefetch ?

Que sont les fichiers Prefetch ?

Dans le cadre de ses analyses, le CERT-FR est régulièrement amené à analyser les fichiers Prefetch, si ceux-ci sont disponibles, afin de déterminer la date d'exécution d'un programme.

Un mot sur les fichiers Prefetch

Dans le cadre de ses analyses, le CERT-FR est régulièrement amené à analyser les fichiers Prefetch, si ceux-ci sont disponibles, afin de déterminer la date d'exécution d'un programme sur le système et éventuellement l'emplacement depuis lequel il a été exécuté.
Pour rappel, les fichiers Prefetch *.pf, introduits sous Windows XP et localisés dans %SystemRoot%Prefetch, sont utilisés par le système d'exploitation pour caractériser les applications exécutées par le système et l'utilisateur.
Cette fonctionnalité permet de déterminer les pages mémoires de code utilisées par un programme afin de les charger préalablement lors de l'exécution de ce dernier. L'objectif ainsi visé est d'éviter un maximum d'accès disque. Par défaut, le Prefetch est désactivé pour tous les programmes sur les environnements Windows Server.

Ce paramètre est stocké dans la valeur suivante :
HKLMSYSTEMCurrentControlSetControlSession ManagerMemory Management
PrefetchParametersEnablePrefetcher
Windows Vista et SuperFetch

Introduit avec le noyau de Vista, SuperFetch est un procédé de gestion de la mémoire, à l'image du Prefetcher introduit sous XP. SuperFetch vise à améliorer les performances générales du système via un mécanisme de prédiction d'utilisation des pages mémoire de code en fonction de scénarios temporels (exécution en semaine ou week-end, utilisation entre 6 heures et midi, midi et 18h, 18h et minuit).
Prefetch ne se base que sur l'activité récente du système pour charger préalablement des données. Si une application utilise intensivement la mémoire, l'historique d'utilisation des pages sera faussé. SuperFetch tente d'optimiser ce modèle de gestion mémoire par le composant de rééquilibrage (rebalancer), qui permet de prioriser à nouveau la liste des pages mémoire en fonction de leur historique d'utilisation et des scénarios temporels établis.
Les fichiers Ag*.db constituent une base d'informations sur l'historique d'utilisation des programmes et de leurs pages mémoire de code. Par abus de langage, ils sont nommés fichiers SuperFetch, bien que ce terme englobe le procédé de gestion mémoire optimisé dans son ensemble. A l'instar des fichiers Prefetch, ils se trouvent dans le dossier %SystemRoot%Prefetch.
Comme pour Prefetcher, le SuperFetch est désactivé par défaut pour tous les programmes sur les environnements Windows Server.

Le paramètre est contenu dans la valeur suivante :
HKLMSYSTEMCurrentControlSetControlSession ManagerMemory Management
PrefetchParametersEnableSuperfetch

Initialement, enablePrefetcher et enableSuperfetch étaient désactivée par défaut sur Windows 7 sur les systèmes équipés de disques SSD, afin d'améliorer la durée de vie des premiers modèles de disque. L'option enablePrefetcher a été réactivée par défaut à partir de Windows 8, mais ce n'est pas le cas pour SuperFetch.

Utilité des artefacts d'exécution de programme

Dans le cadre d'une investigation lors d'un incident de sécurité informatique, l'analyste sera intéressé de savoir si un programme a été exécuté (le nombre de fois, la date, la fréquence et l'emplacement). Cela peut mettre en avant un comportement malveillant si une application suspecte est utilisée, ou déterminer la légitimité d'une autre par une étude statistique.

Les fichiers Prefetch peuvent être décodés avec les outils suivants :
Pf de TzWorks (payant) ;
CrowdResponse de CrowdStrike (gratuit) ;
Windows file analyzer de Mitec (gratuit) ;
le greffon prefetch de RegRipper (libre et gratuit) ;
Prefetch-parser de Airbus DS (libre et gratuit).

Les fichiers SuperFetch peuvent être partiellement décodés avec les outils suivants :
CrowdResponse de CrowdStrike (gratuit) ;
Superfetch-dumper de Rewolf (libre et gratuit).

Documentation
http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-037
http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-044
https://technet.microsoft.com/en-us/magazine/2007.03.vistakernel.aspx
https://www.crowdstrike.com/blog/crowdresponse-application-execution-modules-released
M. Russinovitch, D. Solomon, A. Ionescu. Windows Internals vol.2. Microsoft Press. p.338
https://github.com/libyal/libagdb/blob/master/documentation/Windows SuperFetch (DB) format.asciidoc

---

Réagissez à cet article

Source : *Bulletin d’actualité CERTFR-2015-ACT-051*