Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 01 juin 2015
N° CERTFR-2015-ACT-022

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-022

1 - System Monitor 3

L'utilitaire SysMon (*System Monitor*) est fourni par Microsoft dans sa suite logicielle SysInternals. Il a récemment été mis à jour avec la publication de la version 3. Cet outil permet d'enregistrer dans les journaux d'événements du système de nombreuses informations qui pourront se révéler utiles lors de l'analyse d'un incident de sécurité informatique. L'utilitaire peut être configuré pour se lancer dès le démarrage de la machine, afin de scruter les actions réalisées très tôt lors du démarrage. Les événements suivants sont journalisés :

- la création et la terminaison de processus ;
- le chargement de pilotes de périphériques ;
- le chargement de bibliothèques dynamiques par les processus ;
- la création de fils d'exécution dans des processus tiers via les API `CreateRemoteThread` (nouveauté de la version 3) ;
- le changement de l'attribut « date de création » de fichiers sur le disque ;
- les connexions réseau initiées par les processus.

Ces fonctionnalités peuvent apparaitre similaires à la fonction `Audit process tracking` fournie de base par le système d'exploitation, cependant SysMon apporte des précisions supplémentaires. Il stocke en particulier l'intégralité de la ligne de commande utilisée pour lancer un processus, et calcule un condensat cryptographique des fichiers exécutables considérés. Il permet également de croiser les différents éléments journalisés par l'utilisation d'un `GUID` reliant de façon fiable chaque évenements à un processus.

Toutes ces informations peuvent fournir une aide précieuse lors de l'analyse d'une compromission, ou lors de l'étude d'un code malveillant.

Documentation

- SysMon :
  https://technet.microsoft.com/en-us/sysinternals/dn798348
- Bulletin d'actualité du CERT-FR du 22 août 2014 :
  http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-034

2 - Vigilance sur la catégorisation des sites Internet

La plupart des serveurs mandataires filtrants disposent d'une liste plus ou moins conséquente de catégories dans lesquelles sont classés les sites web. Cette catégorisation est dans la majorité des cas le résultat d'un algorithme mis au point par l'éditeur de la solution de filtrage, avec en complément des vérifications ou ajustements manuels.

L'intérêt de classifier les sites web permet à un administrateur de filtrer les accès en se basant sur des catégories, sans avoir à établir et maintenir lui-même une liste de sites. Ce filtrage peut s'effectuer en liste blanche ou liste noire.

Il faut toutefois rester vigilant et ne pas se reposer uniquement sur cette fonctionnalité pour assurer la protection de son système d'information (stratégie de défense en profondeur). En effet, ces technologies ont certaines limites :

- la catégorisation est faite automatiquement dans la plupart des cas, et même en cas de vérification manuelle, une erreur de catégorisation ou une catégorisation multiple aura pour effet de contourner la politique de sécurité ;
- tous les sites ne sont pas catégorisés, ce qui rend la mise en oeuvre de la liste blanche parfois chronophage auprès des utilisateurs ;
- les domaines malveillants ou les points d'eau sont très volatiles et leur identification auprès de l'éditeur peut prendre un certain temps. Par conséquent, en cas de blocage des catégories liées à du code malveillant (kits d'exploitation, serveurs de contrôle, etc.), des domaines non catégorisés pourront toujours contourner la politique de sécurité pendant une période de temps donnée.

Si cette fonctionnalité est retenue, le CERT-FR recommande de mettre en oeuvre d'autres mécanismes de sécurité en complément, comme ceux présentés dans le guide d'hygiène informatique (pare-feu périmétrique, mise à jour des systèmes, etc.).

Documentation

- Guide d'hygiene informatique
  http://www.ssi.gouv.fr/hygiene-informatique

3 - Rappel des avis émis

Dans la période du 25 au 30 mai 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-237 : Vulnérabilité dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-238 : Vulnérabilité dans le noyau Linux Red Hat
- CERTFR-2015-AVI-239 : Multiples vulnérabilités dans PostgreSQL

Gestion détaillée du document

01 juin 2015 version initiale.