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 18 juillet 2016
N° CERTFR-2016-ACT-029

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-029

1 - Collecte d'artefacts dans le cadre de l'investigation numérique à grande échelle

Introduction

Le CERT-FR est régulièrement amené à traiter des incidents de sécurité informatique de grande ampleur. Il s'agit bien souvent de vérifier la présence actuelle ou passée d'un attaquant sur un système d'information et ceci à partir d'une analyse complète ou par échantillon du parc visé. Cette analyse inclut bien souvent plusieurs milliers de machines (poste de travail ou serveur). Il n'est souvent pas possible de réaliser une analyse disque par disque de l'ensemble d'un parc, c'est pourquoi l'analyste s'attarde bien souvent à quelques artefacts intéressants. Ces derniers visent à détecter les comportements malveillants évoqués dans les bulletins CERTFR-2014-ACT-037 et CERTFR-2015-ACT-038.

Collecte d'artefacts systèmes

Afin de limiter les possibilités de détournement en cas d'infection de la machine collectée, il est préférable de procéder à une collecte de ces éléments directement en utilisant le périphérique PhysicalDrive en lecture seule, sur lequel sont stockées les données concernées. Ce choix est évidemment à adapter à la situation et surtout à la présence ou non de chiffrement entier de partition. Afin de limiter l'empreinte de l'outil sur le système faisant l'objet d'une collecte, il convient également de limiter au maximum le traitement de la donnée sur le système en cours d'exécution (rechercher un marqueur, calculer un condensat, analyser un fichier ou une structure en mémoire, etc.).

Voici une première liste d'artefacts système que l'analyste peut de récupérer pour démarrer son investigation :

- la MFT brute de chaque volume NTFS constituant le catalogue de tous les fichiers présents sur le système avec plusieurs dates et certains attributs spéciaux
- les ruches SYSTEM, SOFTWARE, SAM et Amcache.hve du poste contenant la configuration générale du système et des programmes ainsi que des informations sur l'utilisateur
- les ruches NTUSER.dat et UsrClass.dat de chaque utilisateur possédant un profil sur le poste, contenant la configuration des programmes et les préférences de chaque utilisateur
- les journaux d'évènements Windows (EVT et EVTX) contenant l'historique de l'activité du système : authentifications, bogues, exécutions de programmes, connexions de périphériques, etc.
- le journal de transaction USN de chaque volume NTFS
- les fichiers Prefetch et Superfetch
- les artefacts des navigateurs Web de tous les navigateurs présents (cookies, historiques de navigation et de téléchargement, liste des greffons installés)
- les fichiers "Jump Lists" .automaticDestinations-ms et .customDestinations-ms
- les fichiers RecentFileCache.bcf

- les fichiers LNK de raccourcis
- les fichiers de journalisation générés par le système : mrt.log , windowsupdate.log, setupapi.log
- les journaux antivirus
- les fichiers de miniatures (thumbnails)
- le contenu des corbeilles de chaque volume NTFS
- les 512 premiers octets du disque dur sur lequel la partition système est présente ainsi que les 512 premiers octets de chaque partition NTFS, afin de récupérer le Master Boot Record
- les fichiers BMC de cache des connexions RDP (cf. CERTFR-2016-ACT-017)
- les fichiers de tâche planifiée
- les GPO additionnelles et les scripts lancés au démarrage et à l'arrêt de la machine
- la configuration de chaque carte réseau
- la liste des périphériques connectés à la machine
- la liste des VSC (Volume Shadow Copies)

Collecte d'éléments complémentaires

Enfin, certains types de codes malveillants étant présents uniquement en mémoire, il est parfois utile de collecter des données issues du système en cours d'exécution directement dans la mémoire :

- liste des connexions réseaux actives et les traces des anciennes connexions
- liste des processus en cours d'exécution et des librairies chargées
- liste des services en cours d'exécution
- liste des pilotes chargés et déchargés
- liste des canaux nommés (named pipes)
- liste des mutexes

Le CERT-FR rappelle qu'il est toujours opportun de collecter un certain nombre de journaux issus d'éléments périmétriques, qui vont permettre de faciliter l'investigation :

- les journaux du serveur mandataire
- les journaux du serveur DNS interne
- les journaux du service DHCP
- les journaux des pare-feu et si différents, ceux des serveurs VPN
- les journaux antivirus

Documentation

- Bulletin d'actualité CERTFR-2014-ACT-037
- Bulletin d'actualité CERTFR-2014-ACT-038
- Bulletin d'actualité CERTFR-2016-ACT-017
- R. Rigo. MISC HS n10 nov-dec 2014. Editions Diamond. p.61

2 - Mise à jour mensuelle de Microsoft

Le 12 juillet, lors de sa mise à jour mensuelle, Microsoft a publié onze bulletins de sécurité, dont six sont considérés comme critiques et cinq comme importants :

- MS16-084 (critique) concernant Internet Explorer ;
- MS16-085 (critique) concernant le navigateur Edge ;
- MS16-086 (critique) concernant JScript et VBScript ;
- MS16-087 (critique) concernant les composants de spouleur d'impression Windows ;
- MS16-088 (critique) concernant Microsoft Office ;
- MS16-093 (critique) concernant Adobe Flash Player ;
- MS16-089 (important) concernant le mode de noyau sécurisé de Windows ;
- MS16-090 (important) concernant les pilotes en mode noyau Windows ;
- MS16-091 (important) concernant le cadriciel .NET ;
- MS16-092 (important) concernant le noyau Windows ;
- MS16-094 (important) concernant le démarrage sécurisé.

Navigateurs

Cette mise à jour corrige quatorze vulnérabilités dont sept sont considérées comme critiques dans Internet Explorer. Ces dernières permettent une exécution de code à distance.

Quatre d'entre elles viennent de la manière dont les moteurs de scripts JScript 9 et VBScript traitent les objets en mémoire.

Les trois autres (CVE-2016-3240, CVE-2016-3241, CVE-2016-3242) sont des vulnérabilités d'altération de mémoire dans Internet Explorer.

La vulnérabilité CVE-2016-3243 permet également une exécution de code à distance, celle-ci n'est cependant jugée qu'au niveau importante en raison de sa difficulté d'exploitation.

La vulnérabilité CVE-2016-3245 peut déboucher sur un contournement de la fonctionnalité de sécurité restreignant l'usage d'Internet Explorer vers certains ports. Un attaquant pourrait exploiter la vulnérabilité pour inciter un utilisateur à se connecter à un système distant sur ces ports.

Trois vulnérabilités (CVE-2016-3261, CVE-2016-3273, CVE-2016-3277) sont de type divulgation d'informations, attribuables à un traitement incorrect des objets en mémoire ainsi qu'à une faiblesse du filtre XSS d'Internet Explorer. Les deux autres vulnérabilités (CVE-2016-3274 et CVE-2016-3276) permettent à un attaquant d'usurper l'identité d'un site internet et ainsi paraître légitime aux yeux de l'utilisateur.

Treize vulnérabilités ont été corrigées dans Microsoft Edge, dont sept critiques permettant une exécution de code à distance.

Parmi celles-ci, cinq proviennent de corruptions de mémoire dans le moteur de script Chakra : les CVE-2016-3248, CVE-2016-3259 et CVE-2016-3260 qui touchent également Internet Explorer. Les vulnérabilités CVE-2016-3265 et CVE-2016-3269 sont propres à Edge.

À celles-ci viennent s'ajouter les vulnérabilités CVE-2016-3246 et CVE-2016-3264 qui sont des corruptions de mémoire dans le navigateur.

La CVE-2016-3244 est due à une mauvaise implémentation de la disposition stochastique de l'espace d'adressage mémoire (ASLR), ce qui permettrait à un attaquant de contourner cette fonctionnalité de sécurité pour fiabiliser une éventuelle exécution de code à distance.

Les cinq dernières vulnérabilités sont des vulnérabilités de divulgation d'information et de redirection malveillante et impactent également Internet Explorer.

Dans son bulletin MS-093, Microsoft adresse la cinquantaine de vulnérabilités critiques affectant le Flash Player d'Adobe greffé à ses navigateurs et dont la quasi-totalité permet une exécution de code à distance[1].

Bureautique

Office reçoit sept correctifs de sécurité qui concernent tous des exécutions de code à distance. Quatre d'entre elles sont jugées critiques, trois importantes.

Windows

Outre les vulnérabilités dans les moteurs de script déjà évoquées dans la section Navigateurs, la vulnérabilité CVE-2016-3204 affecte les versions 5.7 et 5.8 de VBScript ainsi que la version 5.8 de JScript. Cette vulnérabilité permet une exécution de code à distance et est jugée critique pour Windows Vista, modérée pour Windows Server 2008.

Les vulnérabilités CVE-2016-3238 et CVE-2016-3239 impactent les composants de spouleur d'impression Windows, et ce sur toutes les versions. L'une permet une exécution de code à distance, l'autre une élévation de privilège. Utilisées conjointement, elles peuvent déboucher sur une compromission totale d'une machine, voire de tout un parc. En effet, à partir du moment où un attaquant arrive à remplacer le pilote d'une imprimante par un fichier malveillant, il peut potentiellement infecter toute machine s'y connectant. Une explication plus détaillée est disponible sur le site de Vectra Networks[2][3].

Les dix autres vulnérabilités affectant Windows permettent principalement des élévations de privilèges ou des fuites d'informations. À noter, la vulnérabilité CVE-2016-3287 permet de contourner le chiffrement de Bitlocker ainsi que la validation de l'intégrité de la séquence de démarrage.

Pour finir, la vulnérabilité CVE-2016-3255 impacte le cadriciel .NET et permet une lecture arbitraire de fichiers lorsqu'une entrée XML contient une référence exploitable vers une entité externe.

Recommandations

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Documentation

1 Bulletin de sécurité Adobe APSB16-25 du 12 juillet 2016
https://helpx.adobe.com/security/products/flash-player/apsb16-25.html
2 Blog Vectra Networks
http://blog.vectranetworks.com/blog/microsoft-windows-printer-wateringhole-attack
3 Vidéo explicative de la vulnérabilité CVE-2016-3238
https://www.youtube.com/watch?v=DuMk-yxZApA

3 - Rappel des avis émis

Dans la période du 11 au 17 juillet 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-227 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-228 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-229 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-230 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-231 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-232 : Vulnérabilité dans Microsoft .NET Framework
- CERTFR-2016-AVI-233 : Multiples vulnérabilités dans Adobe Acrobat et Reader
- CERTFR-2016-AVI-234 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-235 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-236 : Multiples vulnérabilités dans Juniper Junos OS
- CERTFR-2016-AVI-237 : Vulnérabilité dans les produits BlueCoat
- CERTFR-2016-AVI-238 : Vulnérabilité dans le noyau Linux d'Ubuntu

Gestion détaillée du document

18 juillet 2016 version initiale.