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 10 novembre 2014
N° CERTFR-2014-ACT-045

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-045

1 - Vigilance pour le pont du mois de novembre

Ce mardi 11 novembre 2014, Microsoft publiera ses correctifs de sécurité (« patch Tuesday ») pour le mois de novembre. La page *Microsoft Security Advance Notification for November 2014* détaille ces correctifs.

Le CERT-FR souhaite attirer votre attention sur les éléments suivants :

- le nombre inhabituellement élevé de bulletins de sécurité (16) ;
- le niveau de gravité des vulnérabilités corrigées, dont plusieurs sont critiques (exécution de code arbitraire à distance) ;
- les systèmes impactés, en particulier la famille *Windows Server*.

Les serveurs Windows possèdent souvent un, voire des, rôles conséquents sur un réseau. La compromission à distances de ces services peut donc avoir de graves conséquences sur le système d'information.

Dans la mesure où ces correctifs sont publiés un jour férié, le CERT-FR recommande de prendre dès maintenant les dispositions permettant de qualifier et d'appliquer ces correctifs dans les meilleurs délais suite à leur publication.

Documentation

- Microsoft Security Advance Notification for November 2014 :
  https://technet.microsoft.com/fr-fr/library/security/ms14-nov

2 - Nouvelle vulnérabilité impactant OLE

Le 21 octobre 2014, Microsoft a publié un article sur une nouvelle vulnérabilité impactant le composant Office OLE Object (CVE-2014-6352). Le CERT-FR a publié le lendemain l'alerte CERTFR-2014-ALE-009 pour prévenir des risques liés à l'exploitation de cette vulnérabilité.

Selon Microsoft, un attaquant distant pourrait exploiter cette vulnérabilité afin d'exécuter du code arbitraire via un fichier Microsoft Office spécialement formé contenant un objet OLE. Pour rappel, OLE (Object Linking and Embedding) est une technologie qui permet aux applications de partager des données et des fonctionnalités, comme par exemple la capacité de créer et modifier des données composites.

Microsoft indique que la vulnérabilité est actuellement exploitée dans le cadre de campagnes d'attaques à l'aide de fichiers Office PowerPoint malveillants. Cette vulnérabilité est similaire à celle utilisée par la campagne d'attaques « Sandworm » (CVE-2014-4114) et se situe au niveau de la même bibliothèque *Packager.dll*. L'exploitation de cette vulnérabilité repose sur l'utilisation de fichiers *INF* pour télécharger et exécuter une charge malveillante.

Les fichiers *INF* sont des scripts permettant de prendre en charge le lancement d'exécutables. Lorsqu'un object OLE embarque ou fait référence à un fichier *INF*, l'exécutable est lancé par le programme *InfDefaultInstall.exe* sans alerter l'utilisateur. En faisant confiance à un fichier *INF* issu d'une source non sûre, un large vecteur d'attaque

est ainsi créé. Cette vulnérabilité est donc un problème de conception, au même titre que la vulnérabilié CVE-2014-4114. Le problème réside dans la confiance apportée au traitement d'un fichier *INF*.

Cette vulnérabilité n'étant toujours pas corrigée, Microsoft propose un correctif temporaire « Fix it ». Basé sur la technologie Shim, ce correctif bloque l'exécution d'exécutables lancés via un fichier d'information d'installation *INF*.

En attendant un correctif définitif pour la vulnérabilité CVE-2014-6352, le CERT-FR recommande d'appliquer rapidement le contournement temporaire proposé par Microsoft et de ne pas ouvrir de fichiers Office provenant d'une source non sûre.

Documentation

- https://technet.microsoft.com/library/security/3010060
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-009
- https://technet.microsoft.com/en-us/library/security/ms14-060.aspx

3 - Détecter une exfiltration de données

Lors de la compromission d'un parc informatique, il est important pour l'entité visée d'évaluer le contenu ainsi que la quantité des données éventuellement exfiltrées.

Cet article en deux parties a pour objectif de présenter des éléments techniques permettant de repérer les traces de ce type d'opération.

Lorsque l'attaquant a terminé la phase de reconnaissance et a localisé les données d'intérêt (données techniques, données métier, informations à caractère personnel...), il procède généralement à une phase d'exfiltration. Elle peut généralement être divisée en deux : la préparation des données et le transfert de ces données. Cette première partie aborde la détection de la préparation des données.

La préparation des données

Lors de cette première étape, les données ayant été identifiées lors de la phase de reconnaissance sont agrégées puis transformées en vue d'une exfiltration. Ces données peuvent être issues de postes clients, de serveurs ou de partages réseau.

L'agrégation des données

Afin d'identifier les ressources sur lesquelles des données ont pu être agrégées, il convient de rechercher les accès illégitimes à des ressources distantes (cf. le bulletin d'actualité CERTFR-2014-ACT-038).

Dans le cas où l'attaquant aurait utilisé l'explorateur Windows pour réaliser sa collecte, il est possible de déterminer les documents visés à partir des « Shellbags ». Ce sont des données stockées dans la base de registre Windows.

Pour Windows XP on les retrouve sous les clés :

- HKCU\Software\Microsoft\Windows\Shell\Bags
- HKCU\Software\Microsoft\Windows\Shell\BagMRU
- HKCU\Software\Microsoft\Windows\ShellNoRoam\Bags
- HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU

Pour Windows Vista et les versions supérieures :

- HKCU\Local Settings\Software\Microsoft\Windows\Shell\Bags
- HKCU\Local Settings\Software\Microsoft\Windows\Shell\BagMRU
- HKCU\Software\Microsoft\Windows\Shell\Bags
- HKCU\Software\Microsoft\Windows\Shell\BagMRU

Les recherches effectuées via l'explorateur de Windows peuvent être identifiées dans la base de registre :

- (XP) HKCU\Software\Microsoft\Search Assistant\ACMru
- (Vista+) HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Les fichiers accédés via la boîte de dialogue de sauvegarde de Windows sont identifiables dans la clé de registre suivante :

– HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

Les fichiers récemment accédés, présents sous la forme de raccourci et créés automatiquement par Windows, sont identifiables :

– (XP) C:\Documents and Settings\<username>\Recent\
– (Vista+) C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent\
– (Vista+) C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent\

Des logiciels tels que `regripper`, `log2timeline` ou les outils de TZWorks peuvent être utilisés pour rechercher ces « Shellbags ».

La transformation des données

Il est peu fréquent que les données soient envoyées sans modification par l'attaquant. Cela pour plusieurs raisons :

– les données brutes envoyées sur le réseau sont susceptibles d'être détectées par une solution de « prévention de perte de données » ;
– le volume des données à transférer peut être important, il est donc utile pour l'attaquant de les compresser avant exfiltration ;
– l'attaquant a intérêt à chiffrer les données afin de prévenir l'identification des données exfiltrées;
– l'attaquant modifie l'extension des fichiers pour dissimuler la véritable nature des données.

Afin d'identifier les machines ayant servi à la transformation des données, il convient de rechercher les fichiers potentiellement suspects :

– les fichiers effacés ;
– les fichiers caractéristiques d'une archive, ayant les extensions rar, 7z, cab, tar, gz... ;
– les fichiers dont l'extension ne correspond pas aux données du fichier (par exemple, une archive RAR avec une extension jpeg) ;
– les fichiers dont la taille est importante.

L'outil `sorter`, présent dans le logiciel `Sleuthkit`, peut être utilisé pour trier les fichiers d'une image disque en fonction de leur contenu. La sortie de cet outil se présente sous la forme de fichiers textes triés par catégorie (exec.txt, audio.txt, video.txt...). Les fichiers intéressants pour l'analyse d'une exfiltration de données sont les suivants :

– compress.txt : énumère tous les fichiers compressés ;
– archive.txt : énumère tous les fichiers de type archive ;
– crypto.txt : énumère les fichiers chiffrés ou ceux contenant une clé de chiffrement ;
– mismatch.txt : énumère tous les fichiers dont l'extension ne correspond pas aux données.

Pour la compression des données, il est également possible de rechercher la présence sur le disque de traces d'exécution de logiciel connu tel que `WinRAR`, `SevenZip` ou `PowerArchiver`. Le bulletin d'actualité CERTFR-2014-ACT-037 énumère différents artefacts qu'il est possible de trouver suite à l'exécution un programme sous Windows.

Les fichiers présents sur le disque ou ayant été effacés peuvent quant à eux être énumérés par un outil tel que `fls` de la suite `Sleuthkit`. Sur un système de fichiers NTFS, le logiciel `wisp` de TZWorks permet de trouver des fichiers effacés supplémentaires en utilisant des méthodes de « carving ».

La seconde partie de l'article abordera l'étape de détection du transfert des données par l'attaquant.

Documentation

- http://digital-forensics.sans.org/summit-archives/2012/exfiltration-forensics-in-the-age-of-the-cloud.pdf
- http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-038/index.html
- http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-037/index.html
- http://www.cpni.gov.uk/Documents/Publications/2014/2014-04-11-de_lancaster_technical_report.pdf
- https://www.tzworks.net
- http://www.sleuthkit.org

4 - Rappel des avis émis

Dans la période du 03 au 09 novembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-459 : Multiples vulnérabilités dans le noyau linux de Debian
- CERTFR-2014-AVI-460 : Vulnérabilité dans LibreOffice
- CERTFR-2014-AVI-461 : Multiples vulnérabilités dans Cisco Small Business RV Series Routers
- CERTFR-2014-AVI-462 : Vulnérabilité dans Citrix NetScaler

Gestion détaillée du document

10 novembre 2014 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-045`