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 17 novembre 2014
N° CERTFR-2014-ACT-046

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-046

1 - Exfiltration de données (seconde partie)

Cet article est la suite de celui publié la semaine dernière : il se focalise sur la détection du transfert des données au niveau réseau. En effet, 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.

Le transfert des données

La suite de cet article liste les différents moyens généralement utilisés par un attaquant pour exfiltrer les données préparées.

Messagerie

L'attaquant pourra envoyer des données en pièce jointe vers une adresse email qu'il contrôle. Dans le cas d'un service en ligne, des artefacts sont présents dans l'historique de navigation, le cache, les cookies. On pourra aussi retrouver dans les journaux du proxy des requêtes de type POST vers le serveur où les fichiers ont été envoyés.

Service de stockage/sauvegarde en ligne

Les services de stockage ou de sauvegarde en ligne tels que Dropbox, SpiderOak, TeamDrive, ADrive, Carbonite, Mozy Home ou Mozy Stash sont susceptibles d'être utilisés comme moyen d'exfiltration de données. Lors de l'installation de la partie cliente d'un de ces services, puis l'utilisation de celui-ci, un certain nombre d'artefacts sont créés et détectables lors de l'analyse. Le document du SANS *exfiltration forensics in the age of the cloud* présente certains artefacts permettant d'identifier l'exécution d'une de ces applications :

- nom de l'exécutable ;
- dossier d'installation ;
- répertoire de données de l'application ;
- dossier de sauvegarde ou de synchronisation ;
- données de l'application ;
- connexions et signatures réseau ;
- création de clés de registre ;
- artefact restant après installation.

Exfiltration via un programme malveillant

Le plus souvent, les données sont transférées grâce un programme malveillant introduit par l'attaquant. Si le programme malveillant est assez connu (Zeus, PlugX, darkcomet, poison ivy, etc.), l'analyste forensics trouvera des scripts ou de la documentation permettant d'extraire la configuration du programme. Il pourra alors trouver dans cette configuration les domaines ou les adresses IP vers lesquels ont été transférées les données exfiltrées. Ces

éléments pourront par la suite être recherchés dans les journaux proxy afin de retrouver toutes les machines ayant communiqué avec le même serveur de commande et de contrôle. Dans le cas d'un programme malveillant inconnu, les informations sur la configuration pourront être extraites après une analyse approfondie du programme.

Dans certains programmes légitimes, ou même natifs au système tel que netcat ou ftp peuvent aussi servir au transfert des données exfiltrées. Il est donc nécessaire d'identifier toute trace d'exécution de ces programmes.

Supervision des flux IP

Les exfiltrations peuvent faire l'objet d'une détection à travers la supervision des flux IP. La gestion des flux IP est une technologie implémentée sur la plupart des équipements réseau récents (switch, routeur, pare-feu). Ces équipements ont la possibilité d'envoyer des informations, ou métadonnées, sur les flux IP qui les traversent. Il faut pour cela mettre en place un collecteur, qui s'occupera de sauvegarder toutes les informations envoyées par ces différents équipements réseau. Les informations généralement collectées sont les suivantes :

- IP source / destination ;
- port source / destination ;
- durée de la communication ;
- type de protocole ;
- quantité de données ayant transité.

Au cours d'une exfiltration, l'attaquant est susceptible d'être détecté au moment du transfert des données. Il est donc courant lors de cette phase que celui-ci cherche à transférer un maximum d'information en un laps de temps très court. C'est dans ce cas que l'analyse des flux IP apporte des informations importantes sur l'exfiltration. Il est possible selon les cas de rechercher :

- les pics de trafic sur une période d'exfiltration supposée ou sur des créneaux horaires suspects (heures non ouvrées) ;
- l'adresse IP de la machine ayant servi à l'exfiltration afin connaître la quantité de données exfiltrées ;
- les adresses IP des serveurs de commande et de contrôle afin de connaître toutes les machines ayant été utilisées pour l'exfiltration ainsi que la quantité totale des données exfiltrées.

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

2 - Mise à jour mensuelle de Microsoft

Le 11 novembre 2014, lors de sa mise à jour mensuelle, Microsoft a publié quatorze bulletins de sécurité dont quatre sont considérés comme critiques, neuf comme importants et un comme modéré :

- MS14-064 (critique) qui concerne la gestion des objets OLE dans Windows ;
- MS14-065 (critique) qui concerne Internet Explorer ;
- MS14-066 (critique) qui concerne Microsoft Secure Channel ;
- MS14-067 (critique) qui concerne Microsoft XML Core Services ;
- MS14-069 (important) qui concerne Microsoft Office ;
- MS14-070 (important) qui concerne l'implémentation de TCP/IP dans Microsoft Windows ;
- MS14-071 (important) qui concerne le service audio de Microsoft Windows ;
- MS14-072 (important) qui concerne Microsoft .NET ;
- MS14-073 (important) qui concerne Microsoft SharePoint Foundation ;
- MS14-074 (important) qui concerne Microsoft Remote Desktop Protocol ;
- MS14-076 (important) qui concerne Internet Information Services (IIS) ;
- MS14-077 (important) qui concerne Active Directory Federation Services ;
- MS14-078 (important) qui concerne Microsoft Input Method Editor (IME) ;

– MS14-079 (modéré) qui concerne le noyau de Microsoft Windows.

Dans cette mise à jour, un correctif est apporté pour la vulnérabilité concernant le composant Office OLE (CVE-2014-6352) qui avait fait l'objet d'une alerte du CERT-FR (CERTFR-2014-ALE-009). Cette vulnérabilité peut amener à une exécution de code arbitraire à distance.

Internet Explorer fait l'objet de dix-sept vulnérabilités corrigées. L'une d'entres elles (CVE-2014-6323) permet à un site web malveillant d'accéder au contenu du presse-papier de Windows. Les autres vulnérabilités corrigées peuvent amener à un contournement de la distribution aléatoire de l'espace d'adressage (ASLR), une élévation de privilèges ou une exécution de code arbitraire à distance.

La vulnérabilité corrigée dans Microsoft Secure Channel (bibliothèque utilisée pour l'établissement de sessions SSL/TLS) permet une exécution de code à distance due à une erreur lors du traitement de certains paquets. Le CERT-FR insiste sur la criticité de cette vulnérabilité et rappelle qu'une alerte de sécurité la concernant a été émise (CERTFR-2014-ALE-010).

Concernant Microsoft XML Core Services, une vulnérabilité est corrigée. Elle peut conduire à une exécution de code arbitraire à distance si un utilisateur ouvre une page malveillante sous Internet Explorer.

Trois vulnérabilités sont corrigées dans Microsoft Office. Elles peuvent conduire à une exécution de code arbitraire à distance due à une mauvaise manipulation des objets en mémoire.

L'implémentation de la pile TCP/IP dans Microsoft Windows est concernée par une vulnérabilité permettant une élévation de privilèges. Cette vulnérabilité est due à un mauvais traitement des entrées/sorties lors du processus IOCTL. Du code arbitraire peut alors être exécuté dans le même contexte que le processus ciblé et ainsi conduire à une élévation de privilèges selon les droits de ce processus.

Le service audio de Microsoft se voit corrigé d'une vulnérabilité qui peut permettre une élévation de privilèges. En effet, une mauvaise vérification des permissions permet l'exécution de scripts avec des privilèges élevés. Par effet de bord, cela peut être utilisé pour exploiter une autre vulnérabilité permettant l'exécution de code arbitraire.

Une vulnérabilité est corrigée sur Microsoft .NET permettant une élévation de privilèges. Cette vulnérabilité cible les systèmes utilisant le composant ".NET Remoting" (néanmoins, ce composant n'est pas actif par défaut dans les applications basées sur .NET).

De même, une vulnérabilité conduisant à une élévation de privilèges est corrigée dans Microsoft SharePoint Foundation. Pour être affecté, un utilisateur doit visiter un site malveillant spécialement conçu ; un script peut alors être exécuté avec les mêmes droits que l'utilisateur.

Concernant la vulnérabilité Microsoft Remote Desktop Protocol, les tentatives de connexions infructueuses n'étaient pas journalisées. Ainsi, lors d'un audit de sécurité, ces tentatives pourront ne pas être décelées.

La vulnérabilité corrigée dans Microsoft Internet Information Services (IIS) permet de contourner les restrictions mises en place sur les adresses IP ou domaines. Un attaquant peut donc exploiter cette vulnérabilité pour avoir accès à des ressources restreintes.

La mise à jour d'Active Directory Federation Services vise à corriger une vulnérabilité permettant une fuite d'informations. Cette vulnérabilité permet de se reconnecter à une application par navigateur en utilisant les accès d'un utilisateur après que ce dernier se soit déconnecté de cette application.

La vulnérabilité corrigée dans Microsoft Input Method Editor permet une élévation de privilèges par une évasion de l'environnement isolé d'exécution de l'application. L'attaquant peut alors exécuter du code avec les permissions de l'utilisateur connecté. La version japonaise est concernée par cette vulnérabilité.

Enfin, le noyau de Microsoft Windows est vulnérable à un déni de service. Pour cela, l'attaquant utilise un fichier malveillant de police de caractères au format TrueType.

Le CERT-FR rappelle l'importance de certains de ces correctifs de sécurité et recommande ainsi leur application dès que possible.

Documentation

– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ALE-010/index.html
– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-464/index.html
– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-465/index.html
– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-466/index.html
– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-467/index.html
– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-468/index.html
– http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-469/index.html

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-470/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-471/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-472/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-473/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-474/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-475/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-476/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-477/index.html

3 - Rappel des avis émis

Dans la période du 10 au 16 novembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-ALE-010 : Vulnérabilité de l'implémentation des protocoles SSL/TLS dans Microsoft Windows
- CERTFR-2014-AVI-463 : Vulnérabilité dans IBM Tivoli Application Dependency Discovery Manager
- CERTFR-2014-AVI-464 : Multiples vulnérabilités dans Microsoft OLE
- CERTFR-2014-AVI-465 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-466 : Vulnérabilité dans Microsoft Secure Channel (Schannel)
- CERTFR-2014-AVI-467 : Vulnérabilité dans Microsoft XML Core Services
- CERTFR-2014-AVI-468 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2014-AVI-469 : Vulnérabilité dans l'implémentation de TCP/IP dans Microsoft Windows
- CERTFR-2014-AVI-470 : Vulnérabilité dans le service audio de Microsoft Windows
- CERTFR-2014-AVI-471 : Vulnérabilité dans Microsoft .NET
- CERTFR-2014-AVI-472 : Vulnérabilité dans Microsoft SharePoint Foundation
- CERTFR-2014-AVI-473 : Vulnérabilité dans Microsoft Remote Desktop Protocol
- CERTFR-2014-AVI-474 : Vulnérabilité dans Microsoft Internet Information Services (IIS)
- CERTFR-2014-AVI-475 : Vulnérabilité dans Microsoft Active Directory Federation Services
- CERTFR-2014-AVI-476 : Vulnérabilité dans Microsoft Input Method Editor (IME)
- CERTFR-2014-AVI-477 : Vulnérabilité dans le noyau de Microsoft Windows
- CERTFR-2014-AVI-478 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-479 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-480 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2014-AVI-481 : Multiples vulnérabilités dans Wireshark
- CERTFR-2014-AVI-482 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2014-AVI-483 : Multiples vulnérabilités dans PHP

Gestion détaillée du document

17 novembre 2014 version initiale.