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 08 août 2014
N° CERTFR-2014-ACT-032

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-032

1 - Analyse rapide de fichiers suspects (deuxième partie)

Cet article est la suite de l'article [1] publié le 25 juillet 2014 qui a présenté une méthodologie d'analyse rapide des fichiers PE. Cette deuxième partie se concentre sur les fichiers PDF et Office suspects. Une analyse rapide de fichier suspect consiste à déterminer si ce dernier a un caractère malveillant sans en effectuer une analyse approfondie.

Fichiers PDF (Portable Document Format)

Le format PDF est un standard pour les documents élaborés par Adobe dont l'objectif est d'obtenir un affichage identique indépendamment de la plateforme sur laquelle le document est ouvert. Par conséquent, le format ne devrait pas contenir de code exécutable. C'est pourquoi, il y a quelques années, une bonne pratique répandue consistait à transférer des documents sous forme de fichier PDF plutôt qu'Office. Pourtant, depuis 2007 des PDF malveillants sont utilisés pour exécuter du code à l'insu de l'utilisateur et compromettre des machines. Plusieurs raisons expliquent la faisabilité technique :

- Adobe a introduit la possibilité d'insérer du code Javascript dans les documents PDF, et a même étendu le langage. De ce fait, de nombreuses vulnérabilités ont été identifiées dans l'interpréteur Javascript du lecteur Adobe Reader ;
- Adobe Reader utilise des bibliothèques tierces pour gérer certains formats complexes tels que la bibliothèque LibTIFF. Ces librairies peuvent s'avèrer vulnérables ;
- Adobe permet d'embarquer du code Flash dans les documents PDF, et de nombreuses vulnérabilités ont été identifiées dans l'interpréteur Flash ces dernières années.

Comme on peut le voir, la complexification du format PDF a inévitablement ajouté une surface d'attaque importante qui a été mise à profit par les attaquants et les documents PDF sont désormais massivement utilisés pour la compromission de postes distants.

Analyse statique

Un document PDF est structuré sous forme d'objets qui peuvent eux-mêmes référencer d'autres objets, ainsi que d'un en-tête de début et de fin de fichier. Il dispose également d'un index contenant l'emplacement des différents objets dans le document (« `Xref` ») et d'un objet racine (« `Trailer` »), qui pointe vers le premier objet que le lecteur PDF doit ouvrir.

Une des difficultés de l'analyse statique de fichiers PDF est que le lecteur fourni par Adobe est très permissif par rapport aux spécifications du standard. De ce fait, de nombreux outils qui génèrent des PDF ne respectent pas scrupuleusement le standard, et par conséquent il existe de nombreux fichiers PDF malformés et pourtant parfaitement légitimes. Il est donc relativement inutile de rechercher des anomalies par rapport au standard car celles-ci n'indiquent pas forcément un document malveillant. Il est préférable de s'attarder sur les objets qui contiennent des éléments marquants tels que du code Javascript, Flash, ou des images, puisqu'ils peuvent être vecteurs d'exécution

de code. De même, tous les objets permettant le lancement d'une action sont à analyser car ils mènent souvent à un autre objet qui contient du code malveillant.

Un script nommé *PDFiD* [2] permet d'établir un état des lieux des différentes balises trouvées dans un PDF, avec un compteur pour chaque balise. Il permet en un coup d'oeil de voir si du code Javascript est présent dans le fichier PDF, ce qui est peu fréquent pour les documents censés être statiques. Par contre cela est fréquent dans le cas de PDF contenant des formulaires. L'outil recherche également si des balises ont été obfusquées, ce qui est un signe fort de malveillance. Attention toutefois car *PDFiD* effectue une simple recherche de chaînes de caractères mais ne décompresse pas tous les objets de type flux (`Object Stream`), qui peuvent contenir du code malveillant.

Un autre outil nommé *peepdf* [3] permet une analyse beaucoup plus détaillée et dispose en prime d'une base de signatures pour détecter l'exploitation de certaines vulnérabilités connues. Lors de l'ouverture d'un fichier PDF, un résumé d'analyse est affiché avec différentes indications concernant notamment les objets contenant du code Javascript ou des actions d'ouverture automatique, les différentes versions du fichier et la liste des vulnérabilités exploitées. Il est ensuite possible d'extraire le contenu de certains objets pour une analyse plus approfondie ou pour les passer à un moteur d'analyse antivirale.

Les balises suivantes sont à regarder avec une attention particulière :

- `/AA` : « *Automatic Action* », désigne une action qui sera effectuée automatiquement lorsqu'un événement défini après la balise survient ;
- `/OpenAction` : pointe vers un objet qui est accédé lors de l'ouverture du document ;
- `/Javascript` ou `/JS` : balise suivie de code Javascript ou d'un objet contenant lui-même du code Javascript ;
- `/RichMedia` : l'objet associé peut contenir du code Flash.

Une autre vérification rapide qui peut donner des informations intéressantes est l'analyse des métadonnées. Ces champs sont remplis au moment de la génération du document et contiennent des informations telles que la date de création du fichier, l'outil utilisé pour la génération du PDF, le nom de l'auteur, etc. Cependant, ces metadonnées sont parfois utilisées pour stocker du code malveillant obfusqué qui est exécuté via du code Javascript présent dans le PDF. La présence de données incongrues dans ces structures peut être un signe de malveillance. L'outil *exiftool* [4] affiche les métadonnées de différents formats de documents, dont les PDF.

Analyse dynamique

La démarche ici est la même que celle adoptée pour les fichiers PE [1], à savoir une machine virtuelle avec un lecteur Adobe Reader installé. Malheureusement, il est courant qu'un fichier PDF spécialement formé ne déclenche sa charge malveillante que pour une liste définie de versions. Une ouverture du fichier avec une version non ciblée ne provoquera aucune action malveillante visible. Il convient donc de tester le fichier avec plusieurs versions, de préférence de branches différentes puisque certaines fonctionnalités comme le bac à sable n'ont été implémentées qu'à partir de la version 10 du lecteur Adobe Reader.

Concernant les plateformes d'analyse en ligne, *PDF examiner* [5] fournit un rapport avec une partie analyse statique et une partie analyse dynamique. La plateforme Wepawet [6] se concentre plutôt sur le code Javascript présent dans les fichiers PDF.

Fichiers Office

La suite Microsoft Office est assez largement répandue dans les entreprises pour l'édition de documents, ce qui en fait une cible idéale pour l'envoi de documents malveillants. Le format originel (avant Office 2007) s'appuie sur une structure binaire appelée `OLECF` (« *Object Linking and Embedding Compound File* ») ou `Compound Binary File` et nécessite l'utilisation d'outils spécifiques pour parcourir les différentes structures d'un document. Les documents sous ce format ont l'extension .doc (Word), .xls (Excel) ou .ppt (PowerPoint).

Depuis Office 2007, la suite logicielle de Microsoft utilise un format normalisé nommé *Open XML* et les documents produits peuvent être analysés avec des outils standards. L'extension de ces fichiers est .docx, .xlsx et .pptx. Les documents Office offrent également la possibilité d'automatiser des actions grâce à des macros écrites en VBScript. Avant Office 2003, ces macros étaient lancées automatiquement à l'ouverture d'un fichier et présentaient ainsi des risques d'exécution de commandes arbitraires. Les versions suivantes bloquent par défaut les macros non signées. La dernière version d'Office bloque toutes les macros par défaut. Il est à noter que les fichiers au format Open XML contenant une macro doivent obligatoirement avoir l'extension .docm, .xlsm ou .pptm.

Par ailleurs, il est possible d'insérer des fichiers d'un format tiers dans un document Office, comme un exécutable ou un fichier Flash, ce qui rend encore plus difficile le traitement automatisé de ces fichiers. Parfois, sans

être malformé, un document peut embarquer un exécutable et, à partir de techniques d'ingénérie sociale, inciter l'utilisateur à double-cliquer sur celui-ci pour l'exécuter. Pour finir, des vulnérabilités existent dans Microsoft Office et certains documents spécialement formés les exploitent pour exécuter du code arbitraire.

Les risques liés à ce format de document ont été présentés dans un précédent article [7].

Analyse statique

Différents outils d'analyse existent pour chacun des formats évoqués ci-dessus. Ils s'appuient quasiment tous sur une base de données de signatures pour détecter l'exploitation de vulnérabilités connues, mais certains essaient également de détecter des instructions spécifiques à un *shellcode* ou extraient les macros VBA pour permettre leur analyse. L'approche par signature cantonne la détection à des vulnérabilités et méthodes d'exploitation connues.

L'outil *Offvis* [8] dispose de signatures pour des vulnérabilités publiées entre mars 2006 et mai 2009. L'outil *pyOLEScanner* [9] cherche des composants OLE, des *shellcodes* ainsi que des macros dans les documents Office ancienne génération. L'outil *OfficeMalScanner* [10] quant à lui cherche la présence de *shellcodes* et de vulnérabilités connues et donne la possibilité d'extraire les macros d'un fichier Office. Pour finir, l'outil *pyew* [11] liste les structures d'un fichier Office au format binaire. Dans cette liste, on peut identifier des `CLSID` de contrôles ActiveX qui donnent des informations sur le contenu du fichier. Par exemple un document contenant du code Flash aura le `CLSID` « D27CDB6E-AE6D-11cf-96B8-444553540000 ».

Ce même constat peut être établi en analysant les chaînes de caractères d'un fichier Office au format binaire, à la recherche de la chaîne « ShockwaveFlash.ShockwaveFlash ». Le script *xxxswf.py* [12] permet l'extraction des fichiers Flash pour une analyse complémentaire.

Enfin, l'analyse des métadonnées des documents à l'aide d'*exiftool* peut apporter des informations intéressantes. Au-delà du nom de l'auteur et des dates de création et de modification, l'identification d'un encodage de caractères incohérent par rapport à la source du document est un élément suspect.

Analyse dynamique

La problématique de l'analyse dynamique est similaire aux fichiers PDF, car les documents Office malveillants qui cherchent à exploiter une vulnérabilité particulière ne délivreront pas de charge sur une version corrigée ou non vulnérable. Il est donc intéressant de disposer de plusieurs machines virtuelles avec plusieurs versions d'Office et différents correctifs de sécurité. En ce qui concerne les plateformes d'analyse automatique, aucun événement particulier ne sera visible pour les fichiers contenant une charge malveillante dont le déclenchement dépend d'une action utilisateur. A noter que les macros sont éditables directement depuis la suite Office, ce qui permet de les modifier lorsqu'on souhaite effectuer une analyse pas à pas.

Documentation

[1] Analyse rapide de fichiers suspects (première partie) - Bulletin d'actualité CERTFR-2014-ACT-030 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-030/CERTFR-2014-ACT-030.html

[2] PDFiD:
http://blog.didierstevens.com/programs/pdf-tools/

[3] peepdf :
https://code.google.com/p/peepdf/

[4] ExifTool :
http://www.sno.phy.queensu.ca/ phil/exiftool/

[5] PDF Examiner :
http://pdfexaminer.com

[6] Wepawet :
https://wepawet.iseclab.org

[7] Risques liés aux formats Microsoft Office et recommandations - Bulletin d'actualité CERTFR-2014-ACT-012 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-012/CERTFR-2014-ACT-012.html

[8] OffVis :
http://go.microsoft.com/fwlink/?LinkId=158791

[9] pyOLEScanner :
https://github.com/Evilcry/PythonScripts/raw/master/pyOLEScanner.zip

[10] OfficeMalScanner :
http://www.reconstructer.org/code/OfficeMalScanner.zip
[11] Pyew :
http://code.google.com/p/pyew/
[12] xxxswf.py :
http://hooked-on-mnemonics.blogspot.com/2011/12/xxxswfpy.html

2 - Sortie d'EMET 5.0 en version stable

Présentation

Cet article revient sur l'annonce par Microsoft de la sortie de la version 5.0 d'EMET en version stable. Une présentation plus complète de cet outil avait été réalisée à l'occasion du bulletin d'actualité du 7 mars 2014.

Nouvelles fonctionnalités

En plus des fonctionnalités précédemment décrites permettant de réduire la surface d'attaque (Attack Surface Reduction ou ASR) et de renforcer le filtrage des accès à la table d'export (Export Address Table Filtering Plus ou EAF+), plusieurs améliorations sont au rendez-vous.

Une nouvelle fonctionnalité permet de configurer les règles de blocage de certificats en mode strict pour Internet Explorer. Cela permet de bloquer les connexions SSL/TLS dans le cas où le certificat est compromis.

Un travail de fond a également été mené afin de renforcer la résilience d'EMET face aux tentatives de contournement qui avait été employées avec la version 4. Cette nouvelle version apporte aussi une stabilité accrue et une réduction du nombre de faux-positifs.

Conclusion et recommandations

Comme évoqué dans le précédent bulletin d'actualité, EMET représente un moyen simple et efficace de durcir un système même si des techniques de contournement ne sont pas à exclure. En effet, l'installation d'EMET ne dispense pas d'appliquer les mesures recommandées dans le guide d'hygiène informatique.

La version 5.0 d'EMET étant aujourd'hui disponible, le CERT-FR recommande son installation. Il est recommandé de le déployer sur un environnement de test afin de juger de son impact sur les applications métier avant d'envisager son déploiement sur l'ensemble du parc.

Documentation

- Présentation de la trousse à outils EMET par Microsoft :
  https://support.microsoft.com/kb/2458544/fr
- Présentation d'EMET 5.0 par Microsoft :
  http://blogs.technet.com/b/srd/archive/2014/07/31/announcing-emet-v5.aspx
- Bulletin d'actualité 2014-10 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-010/CERTFR-2014-ACT-010.html
- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3 - Changement des mots de passe des comptes d'infrastructure dans l'Active Directory

Contexte

Cette semaine, lors de la conférence BlackHat USA 2014 [1], une présentation abordant la sécurité des Active Directory et du protocole Kerberos a mis en évidence la problématique du non-renouvellement de certains comptes critiques.

Le renouvellement régulier des mots de passe d'un annuaire Active Directory contribue à sécuriser celui-ci en s'assurant, entre autres, qu'un compte compromis ne puisse pas être utilisé très longtemps par un attaquant.

Parmi les différents comptes présents dans un Active Directory figurent plusieurs comptes d'infrastructure dont le mot de passe n'est jamais renouvelé. Deux articles présenteront ces comptes et leur utilité, ainsi qu'une méthode de renouvellement de leur mot de passe. Ce premier article s'intéresse au compte `krbtgt` et un second portera sur les comptes des relations d'approbation (*trust account*).

Le compte `krbtgt` est un compte utilisateur, désactivé par défaut, servant de support de stockage, dans ses attributs, aux clés des centres de distribution de clés Kerberos (appelées clés K_KDC dans la suite). Ces clés sont notamment mises en œuvre afin d'offrir, via Kerberos, un mécanisme d'authentification centralisé permettant de contrôler l'accès aux différents services et ressources en environnement Windows.

Ces clés K_KDC sont calculées à partir d'un mot de passe généré aléatoirement par l'Active Directory dans le but de garantir leur qualité cryptographique. Elles sont la « matière première » cryptographique de toutes les clés Kerberos mises en œuvre pour protéger les tickets émis pour le domaine.

La compromission des clés K_KDC permet à un attaquant de forger des tickets Kerberos de type TGT (*ticket granting ticket*) et ainsi de pouvoir s'authentifier auprès de n'importe quelle ressource (serveur, poste de travail, etc.) du domaine Active Directory avec des droits d'administration.

Le mot de passe du compte `krbtgt` n'est pas changé de manière automatique et les clés K_KDC ne sont donc jamais renouvelées. Le seul changement prévu du mot de passe de ce compte intervient lors de l'augmentation du niveau de fonctionnalités d'un domaine à 2008 ou supérieur afin de générer les clés K_KDC de type AES associées au compte.

Si la base des comptes de l'Active Directory a été extraite (par exemple par un ancien administrateur lors d'un audit ou pour un test de robustesse des mots de passe), il est possible, plusieurs années après, d'utiliser les informations contenues dans la base afin d'en extraire les secrets du compte `krbtgt` et donc les clés K_KDC. Une personne malveillante peut ainsi s'authentifier sur l'ensemble des services du domaine Active Directory des années plus tard même si les mots de passe des comptes utilisateur ont été changés entre temps.

Le CERT-FR recommande ainsi de procéder à un changement manuel du mot de passe du compte `krbtgt`.

La procédure spécifique de changement est décrite ci-dessous. Il est important de noter que, pour être réellement efficace, le changement du mot de passe doit être effectué deux fois. En effet, pour des raisons structurelles, deux générations de mot de passe sont valables pour ce compte.

Dans le cadre d'une forêt mettant en œuvre plusieurs domaines, l'opération de changement de mot de passe doit être effectuée sur chaque domaine de la forêt. Plus généralement, ce changement doit être répété après chaque opération ayant nécessité l'extraction des mots de passe des comptes de l'Active Directory, ainsi que suite au départ d'une personne ayant eu un accès privilégié à la base de comptes de l'Active Directory. Elle peut également être réalisée régulièrement de manière préventive.

Procédure de changement du mot de passe du compte krbtgt

Étape préliminaire

Avant toute opération de changement du mot de passe du compte `krbtgt`, il est indispensable de s'assurer que la réplication des données de l'Active Directory entre les contrôleurs de domaine fonctionne parfaitement.

Microsoft a publié plusieurs documents et méthodologies permettant de s'assurer du bon fonctionnement de la réplication au sein d'un Active Direcory :

- Windows 2003 :
  http://msdn.microsoft.com/fr-fr/library/cc755349.aspx
- Windows 2008/2012 :
  http://technet.microsoft.com/fr-fr/library/cc731170.aspx

Il est également possible d'utiliser l'outil graphique Active Directory Replication Status Tool [2].

Étape 1

Sur le contrôleur de domaine ayant le rôle FSMO (*flexible single master operation*) de *PDC Emulator*, procéder à un premier changement du mot de passe du compte `krbtgt` *via* la commande : `net user krbtgt mdp`

Le mot de passe spécifié (ici « mdp ») peut être totalement arbitraire, le système le remplaçant automatiquement par un mot de passe aléatoire et complexe, indépendant du mot de passe indiqué.

Étape 2

Attendre un certain laps de temps avant de passer à l'étape 3. Ce laps de temps peut être déterminé par deux méthodes différentes.

Méthode 1 (conseillée car plus rapide) :

Attendre que la réplication des données de l'Active Directory se soit correctement effectuée sur chaque contrôleur de domaine avec un compte administrateur de domaine. Pour cela, utiliser par exemple la commande suivante :

```
repadmin /showrepl
```

Vérifier, pour chaque partition (« INSTANCES VOISINES ENTRANTES ») devant être répliquée, que la dernière tentative a réussi à une date postérieure au changement du mot de passe du compte `krbtgt` de l'étape 1. Il est également possible de forcer la vérification sur tous les domaines en exécutant la commande suivante avec un compte administrateur d'entreprise :

```
repadmin /showrepl *
```

En cas d'échec de réplication, le problème doit impérativement être corrigé avant de passer à l'étape 3. Une fois que toutes les réplications se sont correctement déroulées postérieurement au changement du mot de passe du compte `krbtgt`, attendre que tous les TGT expirent. Par défaut, la durée de vie des TGT est fixée à 10 heures.

Méthode 2 (méthode plus longue) :

Attendre 40 jours. Ce délai est suffisamment grand pour s'assurer que la réplication s'est théoriquement effectuée correctement sur tous les contrôleurs de domaine.

Étape 3

Procéder à un second changement du mot de passe du compte `krbtgt` en rejouant l'étape 1.

Documentation

[1] BlackHat USA 2014 :
https://www.blackhat.com/us-14/archives.html
[2] Active Directory Replication Status Tool :
http://www.microsoft.com/en-us/download/details.aspx?id=30005

4 - Rappel des avis émis

Dans la période du 01 au 07 août 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-336 : Multiples vulnérabilités dans IBM WebSphere Portal
- CERTFR-2014-AVI-337 : Vulnérabilité dans IBM Tivoli Network Manager
- CERTFR-2014-AVI-338 : Multiples vulnérabilités dans Wireshark
- CERTFR-2014-AVI-339 : Vulnérabilité dans Samba
- CERTFR-2014-AVI-340 : Vulnérabilité dans Huawei HiLink
- CERTFR-2014-AVI-341 : Vulnérabilité dans les produits Cisco
- CERTFR-2014-AVI-342 : Multiples vulnérabilités dans WordPress
- CERTFR-2014-AVI-343 : Vulnérabilité dans Drupal
- CERTFR-2014-AVI-344 : Multiples vulnérabilités dans OpenSSL

Gestion détaillée du document

08 août 2014 version initiale.