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 26 décembre 2016
N° CERTFR-2016-ACT-052

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-052

1 - Vague d'hameçonnage ciblé utilisant Flash Player et Microsoft Office

Dernièrement, le CERT-FR a constaté de nombreuses vagues d'hameçonnage ciblé exploitant des vulnérabilités du logiciel Flash Player. La particularité de ces vagues réside dans le fait que les objets Flash malveillants sont inclus dans des documents bureautiques, là où il est plus usuel de le voir inclus dans des pages Web.

À cette occasion, le CERT-FR attire l'attention sur le fait qu'il est possible d'exploiter des vulnérabilités ciblant Flash Player à travers des vecteurs moins conventionnels que les navigateurs Web.

Campagnes d'hameçonnage ciblé utilisant Flash à travers un fichier RTF

Depuis le début du mois de novembre 2016, le CERT-FR observe une recrudescence de courriels dont la malveillance est basée sur une pièce jointe de type RTF contenant un objet Flash. Cette vague s'inscrit à la suite de nombreuses autres du même genre depuis plusieurs mois.

Dans le cadre de cette campagne d'attaque, le vecteur utilisé pour la prise de contact et la primo-infection est un courriel invitant son destinataire à ouvrir une pièce jointe au format RTF. Dans la majorité des cas, cette pièce jointe se termine avec l'extension `.doc` mais il s'agit bien d'un fichier au format RTF. Cela conduit à l'ouverture du fichier avec Microsoft Word plutôt que Wordpad, configuré comme lecteur RTF par défaut sur le système d'exploitation Microsoft Windows.

Le format RTF est un format de fichier intermédiaire entre le texte brut et le fichier issu de logiciels de traitement texte évolués. Il permet la rédaction de textes enrichis sans pour autant être aussi complexe que les formats avancés tels que DOC ou ODT. Un fichier au format RTF peut contenir des objets au format binaire tels que des fichiers Flash.

Lors de l'ouverture du document RTF par un logiciel, l'objet binaire est alors lu ou exécuté par le greffon logiciel associé au format. C'est ainsi que les attaquants procèdent pour exploiter une vulnérabilité touchant Flash Player à travers un logiciel comme Microsoft Word.

L'exécution de l'objet Flash se fait en deux temps. En premier lieu, le code Flash agit de façon à dépaqueter un second fichier Flash. Ce second fichier est alors exécuté et réalise certaines opérations réseau afin de prévenir son serveur de commande et de télécharger deux charges utiles au format binaire : la première est un code d'exploitation pour le logiciel Flash Player (CVE-2016-7855) et la seconde est un code encoquillé exploitant une vulnérabilité au sein de Microsoft Windows (CVE-2016-7255) et installant un code malveillant sur la machine. Ce code malveillant est un agent de livraison permettant la compromission à long terme de la machine et utilisé dans le cadre de menaces cybernétiques avancées.

Vecteur d'infection des vulnérabilités Flash Player

Malgré les récentes contre-mesures apportées par Adobe à son logiciel Flash Player (cf. Documentation [1]), celui-ci est toujours une cible de prédilection pour les attaquants qui ont à leur tour adapté leurs techniques. Les tentatives d'infection classiques ciblent directement le logiciel Flash Player à travers le navigateur, mais celles-ci peuvent passer par des documents bureautiques tels que ceux au format Office, RTF ou PDF.

Recommandations

Il est recommandé de désactiver globalement le logiciel Flash Player au sein des logiciels tiers. Le plus simple consiste à désinstaller complètement le greffon du système d'exploitation, mais ceci n'est pas toujours possible en raison des besoins des utilisateurs.

Ainsi, pour désactiver le logiciel Flash Player dans les navigateurs, il faut généralement se rendre dans le gestionnaire de greffons (cf. Documentation [2]).

Comment désactiver les greffons dans le navigateur

Pour désactiver un greffon dans Firefox :

1. aller dans le menu *Outils* puis *Modules complémentaires* ;
2. choisir l'onglet *plugins* ;
3. sélectionner le greffon dans la liste et cliquer sur *Ne jamais activer*.

Pour désactiver un greffon dans Internet Explorer :

1. aller dans le menu *Outils* puis *Gérer les modules complémentaires* ;
2. choisir *Barres d'outils et extensions* ;
3. sélectionner le greffon dans la liste et cliquer sur *Désactiver*.

Cette option peut également être contrôlée via la clé de registre *ActiveX Compatibility* (cf. Documentation [3]).

Pour désactiver un greffon dans Edge :

1. aller dans le menu puis *Paramètres* ;
2. aller dans *Paramètres avancés* ;
3. repérer l'option *Utiliser Adobe Flash Player* ;
4. sélectionner *Désactiver*.

Pour désactiver un greffon dans Google Chrome :

1. saisir `chrome://plugins` dans la barre d'adresse ;
2. sélectionner le greffon et cliquer sur *Désactiver*.

Pour désactiver un greffon dans Safari :

1. aller dans *Préférences* puis *Sécurité* et *Réglages du module externe...* ;
2. décocher la case associée au greffon pour le désactiver complètement, ou sélectionner l'option "Désactivé" qui s'applique lors de l'accès à des sites Web non autorisés explicitement ;
3. valider en cliquant sur *Terminé*.

Pour désactiver un greffon dans Opera :

1. saisir `opera:plugins` dans la barre d'adresse ;
2. sélectionner le greffon puis cliquer sur *Désactiver*.

Active Directory La GPO suivante peut être utilisée pour désactiver le logiciel Flash Player *via* Active Directory : `User Configuration\Windows Components\Internet Explorer\Security Features\Add-on Management`

Pour cela, il faut cliquer sur l'option *Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects* et l'activer en sélectionnant *Enable* (cf. Documentation [4]).

Comment désactiver les greffons dans Microsoft Office

Lors de l'ouverture d'un document par un logiciel de la suite Microsoft Office contenant un objet Flash, l'utilisateur est, par défaut, averti par un message de notification. Par exemple, voici le message provenant de la version 2007 de Word :

This document contains embedded content that may be harmful to your computer.
Choose one of the following options:
Do not allow content to play (Recommended).
I recognize this content. Allow it to play.

Une vigilance particulière doit être apportée à ce message et l'utilisateur est invité à refuser l'exécution.

Pour empêcher automatiquement l'exécution dans les logiciels de la suite Microsoft Office, cette option peut être configurée dans le centre de gestion de la confidentialité (accessible *via* le menu principal). Dans les *Paramètres ActiveX*, il faut sélectionner *Désactiver tous les contrôles sans notification*.

Pour contrôler l'exécution dans tous les documents Office, la fonctionnalité de bit d'arrêt peut être utilisée (cf. Documentation [5]). Pour cela :

- créer un fichier texte `Disable_flash.reg` avec le contenu suivant :

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\
{D27CDB6E-AE6D-11CF-96B8-444553540000}]
"Compatibility Flags"=dword:00000400
```

- dans l'éditeur de base de registre, importer le fichier `Disable_flash.reg`

Comment désactiver les greffons dans Adobe Reader

À l'instar des documents Microsoft Office, lorsqu'un utilisateur tente d'ouvrir un fichier PDF contenant un exécutable Flash, un message de notification est affiché par le mode protégé d'Adobe Reader.

Il est également possible de désactiver explicitement Flash via la clé de registre *FeatureLockDown* :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\<product>\<Version>\FeatureLockDown]
"bEnableFlash" = DWORD:0
```

Documentation

1. http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-040/CERTFR-2015-ACT-040.html
2. http://www.cert.ssi.gouv.fr/site/CERTA-2012-ACT-036/CERTA-2012-ACT-036.html
3. http://www.cert.ssi.gouv.fr/site/CERTA-2010-ALE-007/CERTA-2010-ALE-007.html
4. http://www.tech2tech.fr/comment-desactiver-ou-desinstaller-adobe-flash-sur-tous-les-navigateurs/
5. http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-037/index.html

2 - Rappel des avis émis

Dans la période du 19 au 25 décembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-421 : Vulnérabilité dans SCADA Siemens Desigo PX Web Modules
- CERTFR-2016-AVI-422 : Multiples vulnérabilités dans Squid
- CERTFR-2016-AVI-423 : Multiples vulnérabilités dans Samba
- CERTFR-2016-AVI-424 : Vulnérabilité dans Xen
- CERTFR-2016-AVI-425 : Vulnérabilité dans VMware ESXi
- CERTFR-2016-AVI-426 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-427 : Vulnérabilité dans VMware vSphere Data Protection (VDP)
- CERTFR-2016-AVI-428 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2016-AVI-429 : Vulnérabilité dans Cisco CloudCenter Orchestrator Docker Engine

Durant la même période, les publications suivantes ont été mises à jour :

- CERTFR-2016-AVI-407 : Multiples vulnérabilités dans le noyau Linux de Suse (ajout de nouveaux bulletins de sécurité.)

– CERTFR-2016-AVI-420 : Multiples vulnérabilités dans le noyau Linux de SUSE (ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.)
– CERTFR-2016-AVI-420 : Multiples vulnérabilités dans le noyau Linux de SUSE (ajout de nouveaux bulletins de sécurité et mise à jour des systèmes affectés.)

Gestion détaillée du document

26 décembre 2016 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-2016-ACT-052`