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 14 février 2014
N° CERTFR-2014-ACT-007

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-007

1 - Comptes de service en environnement AD (deuxième partie)

Le premier article de cette série, publié dans le bulletin d'actualité du 31 janvier 2014, a présenté le contexte, les problématiques et les recommandations liés aux comptes de service.

Ce deuxième article décrit différentes techniques permettant d'identifier des comptes de service dans un environnement Active Directory. Elles peuvent être utilisées dans le cadre d'un audit ou d'une démarche de maîtrise des comptes de service dans un système d'information complexe.

Chaque technique permet de récupérer une partie des comptes de service, et ce de manière non exclusive : un même compte peut être identifié par des méthodes différentes. En déroulant toutes les techniques, la liste des comptes de service va se compléter peu à peu.

Au niveau de l'Active Directory

Un moyen simple d'établir une première liste de comptes de service est d'analyser les éléments suivants au niveau de l'Active Directory. Ces éléments ne sont que des pistes qu'il faut investiguer. Leur pertinence dépend des pratiques d'administration et du contexte technique.

Avec des requêtes LDAP, il est possible d'identifier des comptes de service à partir des caractéristiques suivantes :

- l'indicateur `DONT_EXPIRE_PASSWORD` de l'attribut `UserAccountControl` des objets de classe `User` : comme décrit dans l'article précédent, les comptes de service sont souvent paramétrés pour ne pas avoir de renouvellement automatique du mot de passe ;
- le champ de description des objets de classe `User` : certains administrateurs documentent l'usage des comptes dans ce champ ;
- le nom des unités d'organisation (OU) dans lesquelles sont placés les objets de classe `User` : certaines OU sont créées par les administrateurs afin de regrouper les comptes par type ;
- le nom des comptes : une convention de nommage a pu être mise en place afin de classer les types de comptes ;
- les attributs `Service-Principal-Name` (SPN) des objets de classe `User` : dans certains cas, pour que l'authentification avec Kerberos fonctionne, ce champ doit être rempli (automatiquement ou par les administrateurs).

En analysant les paramètres des GPO, il est possible d'identifier les comptes de service à partir :

- des comptes disposant des droits d'authentification `SeServiceLogonRight` (« Ouvrir une session en tant que service ») et `SeBatchLogonRight` (« Ouvrir une session en tant que tâche ») : afin d'être autorisé à s'authentifier sur un poste de travail ou un serveur, un compte de service a besoin d'un de ces droits sur le système concerné ;
- des éventuels comptes utilisés dans des scripts (bat, vbs, ps1, etc.) exécutés dans les GPO.

Au niveau des contrôleurs de domaine

Lors d'une demande de ticket de service Kerberos, un événement *Security/673* (Windows Server 2003) ou *Security/4769* et *Security/4773* (à partir de Windows Server 2008) est généré. Cet événement contient un champ `Service Name` qui indique le compte Active Directory associé au service demandé. Ce compte correspond à un compte machine (se termine par le caractère $) si le service correspondant s'exécute sous l'entité `SYSTEM` ou `NETWORK SERVICE`. Si ce n'est pas un compte de machine, le compte référencé est alors utilisé comme compte de service. Si les journaux des contrôleurs de domaine ne sont pas centralisés et archivés, il est nécessaire d'analyser les journaux de chaque DC. Dans ce cas, l'historique d'événements risque d'être très court et ne permettra de récupérer qu'un nombre limité de comptes de service.

Au niveau des postes et serveurs

Une autre technique d'identification des comptes de service consiste à les chercher sur chaque machine (postes de travail et serveurs) membre du domaine. Cette tâche peut se révéler difficile à réaliser en pratique si aucun outil d'inventaire à distance n'est déployé.

Au niveau de la configuration, les comptes de service peuvent être identifiés parmi :

- les comptes disposant des droits d'authentification `SeServiceLogonRight` (« Ouvrir une session en tant que service ») et `SeBatchLogonRight` (« Ouvrir une session en tant que tâche ») ;
- les comptes du domaine utilisés pour exécuter un service applicatif Windows;
- les comptes du domaine utilisés pour exécuter une tâche planifiée ;
- les comptes du domaine utilisés pour exécuter un composant COM ;
- les comptes du domaine utilisés pour exécuter un Worker IIS.

Au niveau des journaux Windows, les événements *Security/528* (Windows XP/2003) et *Security/4624* (depuis Windows Vista/2008) avec un `LogonType` de valeur 4 ou 5 indiquent qu'un compte a respectivement ouvert une session locale en tant que tâche ou en tant que service. Le paramètre `User Name` désigne alors un compte de service.

Documentation

- Bulletin d'actualité du 31 janvier 2014 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-005.pdf

2 - CryptoLocker

CryptoLocker, un logiciel malveillant de type rançongiciel, a touché de nombreuses victimes depuis sa découverte en septembre 2013. Il se propage principalement par courrier électronique contenant un texte incitant la victime à ouvrir la pièce jointe et à exécuter le logiciel malveillant.

Son objectif principal est de chiffrer certains documents présents sur les disques de sa victime, que ce soit les disques internes ou les disques accessibles par le réseau. Une fois les fichiers chiffrés, le logiciel malveillant incite la victime à payer une rançon (généralement 300 dollars) dans un délai imparti (généralement 72 heures).

La première particularité de ce rançongiciel est l'utilisation de techniques cryptographiques suffisamment avancées pour empêcher la victime de déchiffrer ses documents sans payer la rançon. La deuxième particularité est le recours à un générateur de noms de domaine utilisés pour contacter les serveurs de contrôle et de commande. Ainsi, ces noms de domaines ne sont pas stockés directement dans le code du logiciel, rendant la détection et le blocage de ce code plus complexe.

Fonctionnement de CryptoLocker

Malgré ces particularités, ce rançongiciel dispose des mêmes techniques de propagation et de persistance qu'un code malveillant classique. Au lancement, `CryptoLocker` se copie intégralement dans le dossier temporaire

- `C:\Users\USERNAME\AppData\Roaming\`

La persistance du code est assurée par l'ajout de deux clés de registre dans le profil de l'utilisateur courant :

- `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\`
- `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\`

Une fois la persistance établie sur la machine de la victime, le rançongiciel va utiliser son algorithme de génération de noms de domaine (détaillé dans la section suivante) pour identifier le ou les serveurs de contrôle et de commande avec lesquels il va pouvoir communiquer. Lorsque le serveur a été identifié, `CryptoLocker` demande au serveur de contrôle et de commande la génération d'un couple de clés RSA 2048 bits. La clé privée est stockée sur le serveur tandis que la clé publique est envoyée au logiciel malveillant pour chiffrer les différents fichiers considérés comme importants pour le rançongiciel.

La liste exhaustive des extensions de fichiers recherchées par `CryptoLocker` est présentée ci-dessous :

```
*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps,
*.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb,
*.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd,
*.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr,
*.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw,
*.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw,
*.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c.
```

La sous-clé de registre `HKCU\Software\CryptoLocker\PublicKey` contient la clé publique et la clé de registre `HKCU\Software\CryptoLocker\PublicKey\Files` contient la liste des fichiers qui ont été chiffrés.

Quand le code malveillant a fini de chiffrer tous les fichiers importants des différents disques, une fenêtre s'affiche et indique à la victime la marche à suivre pour payer la rançon.

Algorithme de génération de domaines

L'algorithme de génération de noms de domaines permet de produire périodiquement une liste de noms de domaines (1000 par jour pour `CryptoLocker`). Ces algorithmes sont prédictifs et prennent en paramètre des variables temporelles pour que l'attaquant puisse réserver à l'avance au moins un des noms de domaines qui seront générés. `CryptoLocker` utilise le jour, le mois et l'année actuelle comme graine d'initialisation de son algorithme. La prise en compte de ces trois paramètres permet de générer une liste de noms de domaine prédictive qui changera quotidiennement. Voici quelques exemples de noms de domaine générés par l'algorithme de `CryptoLocker` :

- kdbwveaspxhn.info
- yweffsupuduc.com
- mhyeinfdbclo.net
- ytjhhfcdwwhh.biz
- apesoaoydtnl.ru

Du point de vu de l'attaquant, il lui suffit d'avoir réservé au minimum un nom de domaine par jour (par exemple kdbwveaspxhn.info) et d'attribuer ce nom à l'adresse IP d'un serveur contrôle et de commande de son choix sur la période d'une journée. Le code malveillant génère sa liste quotidienne de noms de domaine et effectue une résolution DNS pour chaque nom de cette liste. Dès qu'un nom de domaine est résolu, `CryptoLocker` récupère l'adresse IP du serveur et communique ensuite de manière classique avec lui (exfiltration d'informations, récupération d'une liste d'actions à effectuer, etc ...).

Pour espérer pouvoir bloquer les communications de ce logiciel malveillant, il serait nécessaire de bloquer la liste complète des domaines qui sont générés par l'algorithme, ce qui reste très difficile à mettre en place en pratique.

Recommandations

- Les attaquants recourent principalement à des techniques d'ingénierie sociale pour inciter leurs victimes à ouvrir les pièces jointes des courriers électroniques émis. Il est donc fortement conseillé de vérifier l'identité de l'émetteur lors de la réception d'un email.
- Faire des sauvegardes régulières permet de réduire les conséquences d'une perte de documents sensibles.
- Avoir un anti-virus avec une base virale à jour permet de détecter la présence de `CryptoLocker`.

Documentation

- Bulletin de sécurité du CERT-FR concernant la nécessité des sauvegardes :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-047.pdf
- Analyse de l'algorithme de génération de nom de domaines de `CryptoLocker` :
  http://blog.fortinet.com/A-Closer-Look-at-CryptoLocker-s-DGA/

3 - Sécurité des données et mobilité

Les médias relatent régulièrement des cas de vol ou d'accès illégitimes à des matériels nomades contenant des données sensibles, notamment à l'occasion de déplacements professionnels ou touristiques. En effet, les données contenues sur des supports amovibles, des ordiphones et des ordinateurs portables sont susceptibles d'être ciblées à des fins d'intelligence économique, d'espionnage, etc.

Afin de se prémunir contre la perte ou le vol de ces supports, le CERT-FR rappelle que l'ANSSI a publié un passeport de conseils aux voyageurs édictant les règles fondamentales à respecter dans le cadre d'un déplacement professionnel, parmi lesquelles :

- utiliser du matériel dédié aux missions ;
- sauvegarder au préalable, les données emportées ;
- ne pas se déplacer avec des données sensibles sans lien avec le déplacement ;
- marquer les appareils d'un signe distinctif discret pour pouvoir détecter les substitutions ;
- utiliser des solutions de chiffrement.

Concernant ce dernier point, le CERT-FR ne peut que recommander l'utilisation des solutions de chiffrement certifiées par l'ANSSI, dans le respect de la législation du pays visité sur l'utilisation de la cryptographie.

Documentation

- Passeport de conseils aux voyageurs :
  http://www.securite-informatique.gouv.fr/partirenmission/
- Législation sur l'usage et l'importation de cryptographie à l'étranger :
  http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs_909/

4 - Rappel des avis émis

Dans la période du 07 au 13 février 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-055 : Multiples vulnérabilités dans Xen
- CERTFR-2014-AVI-056 : Vulnérabilité dans le système SCADA Schneider Electric SCADAPack
- CERTFR-2014-AVI-057 : Vulnérabilité dans Hitachi Cosminexus
- CERTFR-2014-AVI-058 : Vulnérabilité dans le système SCADA Schneider Electric SCADA Expert ClearSCADA
- CERTFR-2014-AVI-059 : Multiples vulnérabilités dans les produits Avaya
- CERTFR-2014-AVI-060 : Vulnérabilité dans Microsoft XML Core Services
- CERTFR-2014-AVI-061 : Vulnérabilité dans la pile IPv6 de Microsoft Windows
- CERTFR-2014-AVI-062 : Vulnérabilité dans Microsoft Direct2D
- CERTFR-2014-AVI-063 : Vulnérabilité dans Microsoft Forefront Protection
- CERTFR-2014-AVI-064 : Multiples vulnérabilités dans Microsoft .NET Framework
- CERTFR-2014-AVI-065 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-066 : Vulnérabilité dans le moteur de script VBScript de Microsoft
- CERTFR-2014-AVI-067 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTFR-2014-AVI-068 : Vulnérabilité dans Apple Boot Camp
- CERTFR-2014-AVI-069 : Multiples vulnérabilités dans les produits Juniper

Gestion détaillée du document

14 février 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-007`