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 19 septembre 2014
N° CERTFR-2014-ACT-038

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-038

1 - Déplacement latéral au sein d'un réseau Microsoft Windows (Seconde Partie)

Cet article fait suite à la publication du 12 septembre 2014 concernant le déplacement latéral d'un attaquant au sein d'un réseau Microsoft Windows. Cette deuxième partie se concentre sur les moyens d'identification des traces d'exécution de code à distance, des accès aux ressources distantes et des connexions utilisateur présentes sur les postes.

Identifier des traces d'exécution de code à distance

Les possibilités d'exécuter du code sur une machine distante sont très nombreuses (services WMI et WinRM, ligne de commandes avancée Powershell, etc.) et chaque solution génère des traces spécifiques. L'analyse des journaux d'évènements et des programmes exécutés sur le poste permettra d'isoler le moyen technique utilisé. Les outils listés ci-dessous sont très fréquemment utilisés dans les compromissions traitées par le CERT-FR.

PsExec de Sysinternals

Cet outil de Microsoft est très largement utilisé. Les différentes traces système présentées dans la première partie de cet article permettront d'attester de son exécution sur la machine hôte. Sur la machine distante, sur laquelle le code est exécuté, des traces sont disponibles dans les journaux d'événements.

Sur un système Vista ou supérieur, la recherche au sein du journal `System` portera par exemple sur les événements 7045 (installation du service `PsExec`) suivis d'un événement 7036 (démarrage du service). S'agissant d'une connexion depuis un poste distant, ces informations pourront être rapprochées des événements liés à l'authentification des utilisateurs (528 ou 4624, « logon » de type 3 ou 2) intervenus juste avant l'installation du service. Ce schéma peut se retrouver également lors de l'utilisation d'autres outils s'appuyant sur un service comme « WCE ».

Tâches planifiées

Une méthode d'exécution de code simple à mettre en oeuvre en utilisant les ressources du système d'exploitation est la création sur la machine distante d'une tâche planifiée pour déployer, par exemple, un malware sur un poste à un instant précis ou lors de la survenance d'un événement prédéfini. L'analyste s'intéressera alors au contenu des fichiers en .job présents dans le répertoire `C:\Windows\Tasks` (XP) ou `C:\Windows\System32\Tasks` (système Vista et supérieurs).

Le fichier `SchedLgu.txt` (XP) et le journal d'événements `Microsoft-Windows-TaskScheduler%Operational.evtx` (systèmes Vista et supérieurs), qui tracent l'exécution des tâches planifiées, doivent également être consultés.

Identifier les accès à des ressources distantes

L'identification des ressources accédées par un attaquant permet de préciser les données et les machines potentiellement compromises.

- Base de registre - Point de montage :
  Enregistrements relatifs aux points de montage liés à un utilisateur. Peut être utile pour isoler des partages réseau accédés par un utilisateur (forme #Serveur#NomDuPartage).
  Emplacement : "ntuser.dat"
  `\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2`
- Base de registre - « Connecter un lecteur réseau » :
  Enregistrements créés lorsqu'un utilisateur affecte une lettre de lecteur à un disque réseau. Cet indicateur est présent sur la machine qui accède au disque réseau. Sur la machine distante hébergeant la ressource, on peut corréler l'information en examinant le journal « Security » à la recherche d'un évènement 4624 (« logon » type 3), sous les systèmes Vista et supérieurs.
  Emplacement : "ntuser.dat"
  `\Software\Microsoft\Windows\CurrentVersion\Explorer\MapNetwork Drive MRU`
- Base de registre - Fichiers récents :
  Pour chaque utilisateur la base de registre conserve des enregistrements relatifs aux documents récemment accédés en local ou sur un serveur distant.
  Emplacement : "ntuser.dat"
  `\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`
- Dossier `RECENT` :
  Ce dossier contient, pour chaque utilisateur, une liste des documents récemment accédés. Au sein des fichiers `*.lnk` il est possible d'extraire le chemin de ressources réseau.
  Emplacement :
  - XP :
    `C:\Documents and settings\[NomUtilisateur]\recent`
  - Vista et supérieur :
    `C:\Users\[NomUtilisateur]\appdata\roaming\microsoft\windows\recent`
- Historique de navigation :
  Les navigateurs Internet peuvent enregistrer, pour chaque utilisateur, l'accès à certains fichiers et notamment des ressources réseau.
  Emplacements :
  - Internet Explorer : fichiers `index.dat` et `WebcacheV0x.dat`
  - Firefox : fichiers `places.sqlite`
- Jumplists : Afin d'améliorer l'expérience utilisateur, les versions récentes de Windows conservent une liste des fichiers récemment accédés par certaines applications pour faciliter l'accès à ces éléments via l'interface graphique. Une liste de fichiers ouverts via l'application est ainsi disponible pour l'analyste.
  Emplacement :
  Systèmes Vista et supérieurs :
  `C:\Users\[NomUtilisateur]\appdata\roaming\microsoft\windows\recent` (fichiers `*Destinations-ns`)

Identifier les connexions utilisateur vers ou depuis le poste compromis

Les possibilités de connexion à distance sur un poste sont multiples (solutions natives Microsoft : RDP, logiciels tiers : UltraVNC, teamviewer, porte dérobée, etc.). Chaque solution génère des traces qui lui sont propres. Seul l'usage de Terminal Service (Remote Desktop Protocol), très fréquemment utilisé, est envisagé ici.

Investigations sur le poste distant

Les éléments suivants peuvent être exploités sur la machine distante où intervient la connexion :

- Journal d'évènements « Sécurité » :
  Identifiants d'évènement XP :
  - 528 (« logon » de type 10 ou de type 2 pour Windows 2000) et 551 (déconnexion) ;
  - 682 (reconnexion) et 683 (déconnexion) ;

Identifiants d'évènement systèmes Vista et supérieurs :
  - 4624 (logon de type 10), 4648, 4634 et 4647 (déconnexion) ;
  - 4778 (reconnexion) et 4779 (déconnexion);
- Journal d'évènements « Terminal-services-RemoteConnectionManager%Operational » :
  Systèmes Vista et supérieurs :
  - 1012 (déconnexion), 1071 (connexion rejetée) ;
  - 1146 et 1147 (ouverture de session), 1148 (échec de l'ouverture de session).

Ces journaux sont stockés aux emplacements suivants :
- XP : `C:\Windows\System32\config`
- Vista et supérieur : `C:\Windows\System32\winevt\Logs`

Investigations sur le poste local

Les éléments suivants peuvent être exploités sur le poste utilisé pour se connecter à une machine distante :
- Base de registre :
  Enregistrements générés lors d'une connexion sur un poste distant via Terminal Service (RDP), contenant la date de la dernière connexion et l'IP de la machine distante.
  Emplacement : "ntuser.dat"
  `\Software\Microsoft\Terminal Server Client\Default` et
  `\Software\Microsoft\Terminal Server Client\Servers`
- Fichiers « *.bmc » :
  Fichiers générés lors de connexions via Terminal Service pour mettre en cache des ressources bitmap. Les images mises en cache peuvent être utilisées pour identifier les machines distantes.
  Emplacements :
  - XP :
    `C:\Documents and Settings\[NomUtilisateur]`
    `\Local Settings\ApplicationData\Microsoft\Terminal Server Client\Cache`
  - Systèmes Vista et supérieurs :
    `C:\Users\[NomUtilisateur]\appdata\local\microsoft\terminal server client\Cache`
- Jumplist :
  L'examen des entrées relatives à Terminal Service permet d'identifier des connexions sur une machine distante.
  Emplacement :
  Systèmes Vista et supérieurs :
  `C:\Users\[NomUtilisateur]\appdata\roaming\microsoft\windows\recent` (fichiers `*Destinations-ns`).

Les outils nécessaires à l'exploitation des traces présentées dans ce bulletin d'actualité sont pré-installés au sein de la distribution forensique « SIFT ») téléchargeable gratuitement à l'adresse http://digital-forensics.sans.org/community/downloads .

2 - Introduction au contrôle d'accès dynamique de Windows

L'augmentation des volumes de données traitées par les systèmes d'information peut nécessiter la mise en place de solutions techniques avancées pour le contrôle d'accès à ces ressources. Dans cette optique, Microsoft a introduit dans Windows 8 et Windows Server 2012 un mécanisme de contrôle d'accès nommé `DAC` (pour « dynamic access control » ou « contrôle d'accès dynamique »). Le `DAC` permet de simplifier la mise en œuvre d'un contrôle d'accès en apportant une classification automatique des données. Cette solution repose sur les revendications (claims) de Windows, des expressions conditionnelles et des règles d'accès centralisées (« central access rule » ou `CAR`). Avant de poursuivre la lecture de cet article, il est recommandé de se référer au bulletin d'actualité 27, publié le 4 juillet 2014, introduisant le contrôle d'accès par revendications de Windows.

Définition

Le contrôle d'accès dynamique comprend un ensemble de mécanismes ayant pour finalité la création de politiques d'accès centrales (« central access policy » ou CAP). Ces éléments sont les suivants :

- des *claims* utilisateur et périphérique;
- des *claims* attributs de ressource;
- des CAR : ce sont des expressions conditionnelles utilisant des opérateurs logiques simples (AND, OR et NOT);
- des CAP : elles sont composées d'une ou plusieurs règles d'accès centrales.

L'administration du contrôle d'accès dynamique, permettant notamment de gérer les politiques d'accès centrales, peut être effectuée par l'intermédiaire du langage de script PowerShell ou par un composant graphique intitulé Active Directory Administrative Center.

Autorisations d'accès

Les CAP représentent un mécanisme de contrôle d'accès supplémentaire complétant les mécanismes existants. Pour rappel, pour un partage de fichiers, il existe deux autres mécanismes historiques de contrôle d'accès :

- les ACL de partage ;
- les ACL sur le système de fichiers NTFS.

Contrairement au contrôle d'accès reposant sur les ACL, le contrôle d'accès CAP ne permet de définir que des règles d'autorisation et pas des règles d'interdiction. Pour autoriser l'accès à une ressource (un fichier par exemple), il est donc nécessaire de satisfaire tous les mécanismes d'autorisation. L'accès ne sera autorisé à un partage réseau que si les politiques Partage, NTFS et Centrale sont activés.

Création d'une politique de contrôle d'accès dynamique

Pour définir une politique d'accès centrale, les étapes suivantes sont nécessaires :

1. création des *claims* (de type utilisateur, périphérique et attributs de ressource);
2. création de règles d'accès centrales utilisant les *claims* précédemment définies;
3. création d'une politique d'accès centrale (CAP) contenant une ou plusieurs règles;
4. activation de la CAP via une stratégie de groupe (GPO);
5. définition manuelle de la CAP à appliquer sur chacune des ressources cibles (*via* les propriétés de sécurité avancées de l'objet).

Exemples concrets

Grâce aux CAP, il est possible de modifier de manière centralisée les règles de contrôle d'accès définies sur un ensemble de systèmes. Par exemple, si l'on souhaite appliquer un contrôle d'accès spécifique à tous les fichiers des dossiers `Anciens projets` et `Projets en cours` (ces dossiers pouvant être présents sur plusieurs serveurs) afin que seuls les utilisateurs français puissent accéder aux documents marqués comme étant en langue française, il est possible de créer un politique d'accès centrale composée de deux règles :

- `@User.country FR`: la *claim* utilisateur ayant pour nom *country* doit avoir pour valeur FR;
- `@Resource.country FR`: l'attribut de ressource *country* du fichier doit avoir pour valeur FR.

Pour être effective, il est nécessaire de procéder aux opérations suivantes :

- l'attribut de ressource *country* doit être défini manuellement sur les dossiers correspondants ;
- la politique d'accès centrale doit être activée *via* une GPO ;
- la politique d'accès centrale doit être positionnée manuellement sur les dossiers correspondants.

Par héritage, la politique est également appliquée à tous les fichiers et sous-dossiers. Dans un deuxième temps, il est décidé que les tous fichiers des dossiers `Anciens projets` et `Projets en cours` (et non plus seulement les fichiers marqués comme étant en langue française) ne peuvent être accédés que par des utilisateurs français. Grâce au contrôle d'accès dynamique, il n'est plus nécessaire de se connecter sur chaque serveur pour modifier des règles d'accès aux ressources. Il suffit de supprimer explicitement la règle `@Resource.country == FR` au niveau de l'Active Directory. Le temps et les efforts demandés pour gérer les accès sont alors considérablement réduits.

Limitation de l'implémentation Microsoft

Il est important d'être conscient que le contrôle d'accès dynamique ne possède pas de mécanisme de cache. Lorsque le lien réseau vers le contrôleur de domaine est coupé, les CAP ne sont plus prises en compte lors du contrôle d'accès. Il est donc déconseillé d'appliquer ce modèle de contrôle d'accès sur des systèmes non maîtrisés d'un point de vue physique et réseau.

Conclusion

Si la mise en place d'une solution de contrôle d'accès dynamique telle que celle proposée par Microsoft demande une préparation et une réflexion conséquentes, la maintenance et les modifications de règles d'accès sont facilitées. Ainsi, le contrôle d'accès dynamique de Windows 8 / Windows Server 2012 marque une première étape vers une plus grande souplesse d'autorisation dans les systèmes Windows. Notons tout de même que ce modèle est conçu principalement pour le contrôle d'accès aux fichiers. L'interface utilisateur ne permet pas d'appliquer une CAP sur des objets autres que des fichiers, bien que cela soit possible via l'utilisation de l'API de programmation Windows.

3 - Mise à jour du gestionnaire de paquets apt

Le 16 septembre 2014, les distributions Linux Debian et Ubuntu proposent une mise à jour de sécurité visant leur outil interne de gestion de paquets « apt ». Cinq failles de sécurité (CVE-2014-0487, CVE-2014-0488, CVE-2014-0489 et CVE-2014-0490) ont été corrigées dans cette nouvelle version et sont toutes en relation avec la vérification des condensats lors de la validation des données téléchargées. Les corrections apportées sont les suivantes :

- CVE-2014-0487 : corrige l'absence de vérification des condensats dans le cas où le paquet du dépôt distant a été précédemment téléchargé localement et que les versions (entre le dépôt distant et le système de fichiers) sont les mêmes. Avec cette correction, le système s'assure que le fichier local n'a pas été corrompu ;
- CVE-2014-0488 : corrige le comportement du code lorsqu'un dépôt passe du statut non authentifié au statut authentifié. Tous les paquets téléchargés avant authentification du dépôt distant sont supprimés ;
- CVE-2014-0489 : corrige le comportement du code lorsque l'option « Acquire::GzipIndexes » par défaut désactivée est précisée. Auparavant, dans le cas où l'option a été définie, le code n'effectuait pas la vérification des condensats ;
- CVE-2014-0490 : corrige le comportement du code lorsqu'un téléchargement de paquets est réalisé manuellement grâce à la commande « apt-get download ». Auparavant, aucune vérification des condensats n'était effectuée. Après cette modification, un message d'erreur est affiché sur la console.

Le CERT-FR recommande donc aux utilisateurs de ces distributions Linux d'appliquer ces mises à jour afin de garantir l'intégrité des paquets qui sont installés sur une machine.

4 - Rappel des avis émis

Dans la période du 12 au 18 septembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-384 : Vulnérabilité dans VMware NSX et vCNS
- CERTFR-2014-AVI-385 : Multiples vulnérabilités dans Moodle
- CERTFR-2014-AVI-386 : Vulnérabilité dans phpMyAdmin
- CERTFR-2014-AVI-387 : Multiples vulnérabilités dans Juniper
- CERTFR-2014-AVI-388 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2014-AVI-389 : Multiples vulnérabilités dans Adobe Reader et Acrobat
- CERTFR-2014-AVI-390 : Multiples vulnérabilités dans Wireshark
- CERTFR-2014-AVI-391 : Vulnérabilité dans le système SCADA Schneider Electric VAMPSET
- CERTFR-2014-AVI-392 : Vulnérabilité dans Nginx
- CERTFR-2014-AVI-393 : Multiples vulnérabilités dans les produits Apple

Gestion détaillée du document

19 septembre 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-038