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 24 août 2015
N° CERTFR-2015-ACT-034

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-034

1 - Détails techniques et configuration des RODC

Dans une première partie de cette série consacrée aux RODC, les bénéfices attendus des RODC avaient été présentés. Ce deuxième article aborde les aspects techniques des RODC et en particulier les différences avec les RWDC. La première partie est disponible à l'adresse :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-032/

Identification des RODC

Tout comme les RWDC, les RODC sont présents dans l'OU `Domain Controllers`, à la racine de la partition du domaine. Cependant, ils sont différenciables par leur attribut `User-Account-Control`, qui possède alors le flag `ADS_UF_PARTIAL_SECRETS_ACCOUNT` (valeur 0x04000000). Le filtre LDAP suivant permet alors d'identifier les RODC d'un domaine :

```
(userAccountControl:1.2.840.113556.1.4.803:=67108864).
```

Attributs LDAP

Une fois identifiés, les objets AD représentant les RODC possèdent plusieurs attributs intéressants, dont les principaux sont détaillés ci-dessous. Ces attributs sont principalement des attributs facultatifs de la classe d'objets `computer` et ne sont utilisés que par les RODC. Ils permettent la configuration des RODC ou donnent des informations sur leur état.

- `managed-By` : désigne un utilisateur ou un groupe possédant la délégation d'administration locale du RODC. Il est particulièrement intéressant puisque cet utilisateur sera (resp. les membres de ce groupe seront) membre implicite du groupe d'administration local au RODC.
- `ms-DS-Revealed-Users` : regroupe la liste des utilisateurs et machines dont les secrets d'authentification ont été révélés au RODC (s'ils l'ont été explicitement autorisés, comme expliqué par la suite). On parle alors d'utilisateurs "mis en cache" sur le RODC.
- `ms-DS-Never-Reveal-Group` : regroupe la liste des entités de sécurité (utilisateurs, machines, groupes) qu'il sera interdit de mettre en cache sur le RODC, c'est à dire dont les secrets d'authentification ne pourront pas lui être révélés. Par défaut, cet attribut contient les groupes bien connus "Builtin Administrators", "Account Operators", "Server Operators" et "Backup Operators", ainsi que le groupe intégré du domaine "Groupe de réplication dont le mot de passe RODC est refusé" (*Denied RODC Password Replication Group*), lui-même contenant les entités très privilégiées du domaine (administrateurs du domaine, du schéma, de l'entreprise, compte krbtgt, etc.). Cet attribut constitue donc la *liste noire* du cache du RODC.
- `ms-DS-Reveal-OnDemand-Group` : regroupe la liste des entités de sécurité autorisées à être mises en cache sur le RODC (dont les secrets pourront lui être révélés). Par défaut cet attribut ne contient que le groupe du domaine "Allowed RODC Password Replication Group", lui-même étant vide par défaut. Cet attribut constitue donc la *liste blanche* du cache du RODC. Cette liste blanche est secondaire par rapport à la liste noire, qui a la priorité dans le cas où une entité figurerait dans les deux listes.

Les deux attributs précédents forment ce qu'on appelle là PRP (*Password Replication Policy*) du RODC, qui définit quelles entités peuvent et ne peuvent pas être mises en cache sur des RODC. Cette PRP est maintenue et validée par les RWDC. Pour tous les RODC, la PRP s'appuie par défaut sur les deux groupes du domaine intégrés "Groupe de réplication dont le mot de passe RODC est autorisé" (*Allowed RODC Password Replication Group*) et "Groupe de réplication dont le mot de passe RODC est refusé" (*Denied RODC Password Replication Group*). Ces groupes, dans leur état par défaut, permettent d'interdire les entités privilégiées sur tous les RODC et de n'en autoriser aucune.

- `ms-DS-KrbTgt-Link` : lien vers l'utilisateur `krbtgt` spécifique au RODC (ayant la forme `krbtgt_<id>`). Chaque RODC possède en effet un compte krbtgt qui lui est propre, et dont il se sert pour chiffrer les tickets kerberos des entités mises en cache dont il dispose des secrets. En effet, lorsqu'un RODC ne possède pas le secret d'un utilisateur ou de la ressource à laquelle il veut accéder, il transmet les demandes de tickets à un RWDC (également pour toute opération d'écriture). Cependant, s'il possède ces éléments, il est alors en mesure de générer des TGT (*Ticket-Granting-Ticket*) et des tickets de service d'accès aux ressources sans contacter de RWDC. C'est ce mécanisme qui permet l'authentification des entités mises en cache même si aucun RWDC n'est disponible (par exemple dans le cas d'un lien réseau coupé).

Filtered Attribute Set

Comme énoncé précédemment, les RODC ne possèdent pas tous les attributs de tous les objets qu'ils répliquent. Un ensemble d'attributs ne leur est jamais transmis : c'est cet ensemble qui constitue le FAS (*Filtered Attribute Set*). Cet ensemble est dynamique, et est constitué de tous les attributs dont l'objet du schéma (de type `Attribute-Schema`) possède le flag `fRODCFilteredAttribute` (valeur 0x200) dans leur attribut `Search-Flags`.

On y retrouve ainsi des attributs concernant le TPM d'une machine (`ms-TPM-OwnerInformation`), les clés maîtres DPAPI d'un utilisateur (`ms-PKI-DPAPIMasterKeys`), les clés de recouvrement BitLocker (`ms-FVE-RecoveryPassword`) ou encore des attributs contenant des mots de passe (`ms-MCS-AdmPwd`, en présence de l'extension de schéma Microsoft LAPS).

À noter que certains attributs ne peuvent pas faire partie de ce FAS, notamment des attributs construits ou des attributs critiques (c'est-à-dire dont l'objet du schéma possède le flag `FLAG_ATTR_IS_CRITICAL` dans leur attribut `Schema-Flags-Ex`), qui seront alors toujours répliqués sur les RODC.

Opérations de réplication

Les RODC ne possèdent pas le droit étendu `DS-Replication-Get-Changes-All` à la racine de la partition de domaine, mais (principalement) le droit `DS-Replication-Get-Changes`. Ils ne peuvent donc pas répliquer les attributs secrets des entités par les mêmes opérations de réplication que les RWDC.

Ils utilisent à la place un "trigger RootDSE" (une opération LDAP particulière effectuée sur le RootDSE, la racine de l'annuaire LDAP) nommée `replicateSingleObject` en spécifiant le DN (Distinguished Name) de l'entité à répliquer et en spécifiant la chaîne "SECRETS_ONLY" pour mettre en cache les secrets de cette entité.

Cette opération à l'initiative du RODC et à destination d'un RWDC n'est validée par ce dernier que si la PRP associée au RODC le permet. Enfin, si elle est normalement déclenchée à l'initiative du RODC, cette opération peut l'être manuellement avec un compte administrateur local d'un RODC, en utilisant par exemple l'outil natif `repadmin` et l'option `/rodcpwdrepl` : il est donc possible pour un administrateur local d'un RODC de forcer la mise en cache de toute la liste blanche de ce RODC (définie par l'attribut `ms-DS-Reveal-OnDemand-Group`).

2 - Conficker

Le CERT-FR a constaté que le ver Conficker (aussi connu sous les noms de Downup, Downadup ou Kido) peut encore être très présent dans un système d'information de grande taille.

Historique

Apparu en 2008, ce ver visant les systèmes d'exploitation Windows s'est rapidement répandu pour atteindre son pic d'activité courant 2009, au travers de nombreuses variantes consécutives [1]. Malgré la prise en compte par les principaux éditeurs antivirus des différentes versions de ce maliciel et la mise en place de serveurs souillards (sinkhole) pour les domaines contactés, ce maliciel est encore très présent en 2015.

Moyens de détections

La présence de Conficker peut-être détectée à plusieurs niveaux. Parmi les méthodes à privilégier, le CERT-FR recommande :

- la mise en place d'un système de détection d'intrusions (IDS) disposant des règles ad hoc. Par exemple, l'IDS Snort permet de réaliser cette détection ;
- la vérification des journaux de connexion, en particulier ceux des systèmes de résolution de nom ou de filtrage à la recherche de domaines contactés par le maliciel ;
- la surveillance des comptes utilisateurs ou administrateurs bloqués de manière régulière. Il peut s'agir de la conséquence d'une attaque en ligne sur les mots de passe ;
- la vérification des accès au service de mise à jour Windows (WSUS ou Windows Update) ou de l'éditeur antivirus.

La détection de Conficker dans un système d'information n'est pas anodine car il reflète d'importantes lacunes dans l'application de la politique de sécurité du système d'information. Des infections par d'autres maliciels (moins populaires) sont très probables.

Se prémunir de l'infection

Au cours des nombreux renouvellements de matériel dans le système d'information depuis 2008, le ver Conficker a pu réussir à se maintenir (ou infecter de nouvelles machines). Dans le cas présent, des règles simples permettent d'éviter une nouvelle infection :

- utiliser un antivirus et le maintenir à jour ;
- mettre à jour l'ensemble de son parc informatique (appliquer notamment le correctif pour la vulnérabilité MS08-67 dans le cas de Conficker)[2] ou migrer vers des versions récentes de Windows ;
- utiliser des mots de passe robustes, conformes aux recommandations en vigueur [3] ;
- désactiver l'ensemble des lecteurs/partages réseau inutiles et/ou accessibles sans authentification ;
- désactiver les fonctionnalités de lancement automatique des programmes (autorun).

Documentation

1 http://www.cert.ssi.gouv.fr/site/CERTA-2009-ACT-013.pdf

2 https://technet.microsoft.com/library/security/ms08-067

3 http://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf

3 - Rappel des avis émis

Dans la période du 17 au 23 août 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-357 : Multiples vulnérabilités dans le noyau Linux de OpenSUSE
- CERTFR-2015-AVI-358 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-359 : Multiples vulnérabilités dans le noyau Linux de Fedora
- CERTFR-2015-AVI-360 : Vulnérabilité dans Citrix XenServer
- CERTFR-2015-AVI-361 : Multiples vulnérabilités dans Symantec Endpoint Protection

Gestion détaillée du document

24 août 2015 version initiale.

Dernière version de ce document : http://cert.ssi.gouv.fr/site/CERTFR-2015-ACT-034