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 22 août 2014
N° CERTFR-2014-ACT-034

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-034

1 - SSTIC 2014 : Chemins de contrôle en environnement Active Directory

Introduction

À l'occasion de la conférence SSTIC 2014, l'ANSSI a réalisé une présentation intitulée « Chemins de contrôle en environnement Active Directory » [1].

Cette présentation découle d'un constat : l'audit d'un domaine Active Directory est un sujet complexe. Les analyses traditionnelles des appartenances aux groupes d'administration ou des permissions sur quelques conteneurs importants sont insuffisantes.

L'ANSSI a ainsi développé une méthodologie et un outillage permettant de prendre en compte et d'agréger de nombreuses relations de contrôle provenant de sources de données variées, telles que :

- les permissions et les propriétés des objets de l'annuaire ;
- l'appartenance aux groupes de sécurité ;
- la hiérarchie des conteneurs de l'annuaire ;
- les objets des stratégies de groupe (GPO) ;
- des données provenant des machines locales, telles que les journaux d'événements.

L'agrégation de ces relations permet de les présenter sous forme de graphes appelés « graphes de chemins de contrôle », afin de représenter graphiquement les réponses à des questions telles que « Qui peut obtenir les privilèges d'administration du domaine ? » ou « Quelles ressources un utilisateur peut-il contrôler ? ».

La première partie de la présentation SSTIC définissait les relations et chemins de contrôle, et abordait l'outillage réalisé. La seconde partie présentait quant à elle des scénarios d'analyse sur plusieurs domaines différents.

Méthode et outils

Les « relations de contrôle » traduisent la maîtrise d'un objet sur un autre. Par exemple :

- la permission de réinitialiser le mot de passe d'un utilisateur ;
- les permissions d'écrire des fichiers de GPO ;
- l'appartenance à un groupe local d'administration d'une machine ;
- la connexion d'un utilisateur sur une machine.

La définition de ces relations nécessite d'inspecter chaque type d'objet considéré (ses attributs, les droits pouvant s'y appliquer, etc.) afin de définir quels sont ceux pouvant avoir un impact sur la sécurité de l'objet.

L'agrégation de ces relations forme ensuite des « chemins de contrôle » qui représentent un enchaînement d'actions permettant de passer d'un noeud à un autre. Ils sont modélisés sous forme de graphe orienté dont les objets sont les noeuds et les relations sont les arcs.

L'outillage présenté réalise ensuite les actions suivantes :

1. la collecte des relations sous forme de fichiers TSV bruts (par exemple au moyen d'accès LDAP pour l'annuaire, ou d'accès aux données de sécurité du SYSVOL pour les GPO) ;

2. l'import dans une « base de données orientée-graphe » (la base de données orientée graphe choisie est Neo4j [2]) au moyen d'un logiciel d'import « à froid » permettant de traiter des volumes de données importants en un temps raisonnable ;
3. le requêtage de cette base et la transformation des résultats pour affichage sous forme visuelle, à l'aide d'une bibliothèque d'affichage (la bibliothèque utilisée pour l'affichage des graphes est D3.js [3]).

Scénarios

À l'aide de l'outillage réalisé, des graphes de chemins de contrôle centrés sur le groupe « `Administrateurs du domaine` » ont été présentés pour différents domaines. Ces graphes permettent de répondre aux questions « Qui peut obtenir les privilèges d'administration du domaine ? », « Qui a accès à des ressources critiques du système d'information ? ».

Le graphe d'un domaine vierge a permis d'identifier les acteurs présents par défaut et d'établir une situation de référence. On retrouve par exemple sur ce graphe des acteurs très privilégiés présents dans tous les domaines (le compte natif « `Administrateur` », les groupes natifs « `Administrateurs` » et « `Administrateurs de l'entreprise` », `SYSTEM`) et des éléments liés à la GPO par défaut (« `default domain policy` »).

Les graphes générés pour des domaines plus complexes permettent d'identifier des situations particulières, telles que des problèmes d'hygiène du domaine, des déviances dans sa gestion, voire des portes dérobées potentiellement laissées par un attaquant après une compromission. La taille des graphes générés, contenant parfois des centaines de noeuds, illustre bien la complexité d'identification d'un périmètre critique d'un domaine.

Conclusion

Ces travaux proposent une nouvelle méthodologie pour l'étude de la sécurité des environnements Active Directory. Elle peut être appliquée dans différents contextes :

- audit, pour durcissement ;
- réponse à incident, après compromission ;
- contrôle régulier de la configuration, pour détecter l'apparition de mauvaises pratiques.

L'outillage réalisé est désormais disponible sur le github de l'ANSSI [4]. Les commentaires et retours d'utilisation seront appréciés par les auteurs.

Documentation

[1] Lien de la présentation (planches et article complet) :
https://www.sstic.org/2014/presentation/chemins_de_controle_active_directory/

[2] Neo4j :
http://www.neo4j.org/

[3] D3.js :
http://d3js.org/

[4] Dépot github de l'outillage réalisé :
http://github.com/ANSSI-FR/AD-control-paths/

2 - System Monitor

System Monitor, ou « Sysmon », est un nouvel outil de la suite *Windows Sysinternals*, maintenu par Microsoft. Cet outil permet d'enregistrer, sous forme d'événements Windows, diverses activités du système. Il présente, en outre, l'intérêt d'être persistant au redémarrage du système.

Trois types d'événements sont journalisés :

1. Les créations de processus :
   - date de création ;
   - chemin du processus ;
   - ligne de commande ayant permis de lancer le processus ;
   - condensé du binaire (MD5, SHA256 ou SHA1) ;
   - chemin du processus parent.

2. Les activités de changement de date de création de fichiers :
   - date de changement ;
   - chemin du fichier ;
   - chemin du processus réalisant l'action.
3. Les connexions réseau TCP et UDP :
   - date de la connexion ;
   - chemin du processus ayant établi la connexion ;
   - adresses IP, ports et noms de machines source et destination.

Ces évènements sont stockés dans les journaux Windows et accessibles depuis l'observateur d'événements de Windows :

- pour les versions de Windows précédant Vista, dans le journal *System*;
- pour Vista et les versions ultérieures, dans *Applications and Services Logs/Microsoft/Windows/Sysmon/Operational*.

Dans le cadre d'une analyse forensics d'un poste Windows, ces éléments apportent des informations supplémentaires précieuses, permettant de comprendre les actions menées par un attaquant ou de suivre l'activité d'un logiciel malveillant.

L'installation de System Monitor sur un parc informatique utilisant des technologies Microsoft, couplée à une gestion saine des journaux d'évènements, facilite le traitement d'investigations numériques.

Documentation

- Outil System Monitor :
  http://technet.microsoft.com/en-us/sysinternals/dn798348.aspx
- Recommandations de sécurité pour la mise en œuvre d'un système de journalisation :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Journalisation_NoteTech.pdf

3 - Rappel des avis émis

Dans la période du 15 au 21 août 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-359 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-360 : Vulnérabilité dans le système SCADA Siemens SIMATIC S7-1500 CPU
- CERTFR-2014-AVI-361 : Vulnérabilité dans Innominate mGuard
- CERTFR-2014-AVI-362 : Multiples vulnérabilités dans EMC Documentum
- CERTFR-2014-AVI-363 : Multiples vulnérabilités dans RSA Archer GRC Platform
- CERTFR-2014-AVI-364 : Multiples vulnérabilités dans les produits IBM
- CERTFR-2014-AVI-365 : Vulnérabilité dans Red Hat JBoss

Gestion détaillée du document

22 août 2014 version initiale.