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 13 juin 2014
N° CERTFR-2014-ACT-024

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-024

1 - Journalisation des flux réseau (première partie)

Le CERT-FR constate, au travers des incidents traités, qu'il est indispensable de collecter et conserver un maximum de données sur l'activité d'un système d'information pour traiter au mieux un incident de sécurité informatique. A ce titre, les flux réseau sont une source primordiale d'information.

Cependant, plusieurs points sont à prendre en compte lors de la conception d'une politique de journalisation de ces flux. En effet, pour que ces journaux soient pertinents dans le cadre d'un traitement d'incident, ils doivent permettre d'identifier précisément la source et la destination d'un flux réseau et contenir les informations nécessaires permettant de le qualifier.

Une politique raisonnable d'archivage de ces journaux doit également être décidée. Le cadre légal va aussi influer sur les données pouvant être collectées et conservées. L'ANSSI a publié une note sur la mise en œuvre d'un système de journalisation qui précise les aspects juridiques et réglementaires, dans l'Annexe C.

Identifier la source et destination d'un flux réseau

Lors du traitement d'un incident de sécurité, la victime doit être en capacité d'identifier les machines compromises ou cibles d'attaque en recherchant les marqueurs de comportements malveillants dans ses journaux. Pour cela, il est indispensable de s'assurer que des informations d'identification sont présentes dans tous les journaux des équipements réseau ou applicatifs, par exemple :

- l'adresse électronique du destinataire de courrier électronique ;
- le compte de l'utilisateur authentifié auprès des serveurs mandataires HTTP ;
- l'adresse IP à l'origine de la connexion bloquée dans les journaux pare-feu.

Une politique de journalisation des flux réseau est efficace si au moins un des équipements sur le chemin du flux permet d'en assurer une journalisation suffisamment fine. Un cas classique rencontré par le CERT-FR est la recherche de postes compromis par un code malveillant communiquant avec un serveur de commande et de contrôle par navigation Web sur des domaines connus.

Si une chaîne de serveurs mandataires HTTP est mise en place pour filtrer la navigation, chacun des équipements devra journaliser les adresses IP source et destination des requêtes. De plus, si le serveur mandataire se situe après un équipement réseau réalisant de la traduction d'adresse IP (NAT), il sera également nécessaire que cet équipement journalise les requêtes. Faute de quoi l'identification des postes à l'origine de la requête sur le domaine malveillant sera impossible.

La nature dynamique d'un système d'information est aussi une chose à prendre en compte lors de l'établissement d'une politique de journalisation. Par exemple, si l'IP de la machine est choisie en tant que moyen d'identification dans les journaux, il est indispensable de conserver les journaux DHCP. Un prérequis à la mise en place d'une politique de journalisation est de posséder une connaissance suffisante du système d'information, et nécessite donc l'établissement d'une cartographie à plusieurs niveaux (applicatifs, réseaux, etc.) du système d'information.

Caractériser un flux

Au delà des informations permettant d'identifier le poste source et la destination d'un flux, d'autres caractéristiques propres à ce flux peuvent faciliter le traitement d'un incident.

Niveau réseau

L'exploitation des journaux ne peut être efficace que s'ils contiennent a minima les informations suivantes :

- adresse IP source ;
- adresse IP destination ;
- heure et date de la connexion ;
- ports source et destination ;
- volumes de données échangées (envoyés et reçus).

Ces données peuvent être récoltées sur la plupart des équipements réseaux (commutateurs, routeurs, etc.). Dans le cas contraire, le CERT-FR recommande la mise en place de sondes tierces afin de pallier les défauts de journalisation de ces équipements. On pourra par exemple déployer des sondes génératrices de flux (de type *netflow*, *IPFIX*, etc.).

L'exploitation de ces journaux permet d'identifier des flux réseau anormaux. Par exemple, un important volume de données sortant à des heures non ouvrées peut être caractéristique d'une exfiltration. Une augmentation importante de la quantité de données véhiculées sur un port particulier peut également traduire un comportement illégitime. Ainsi un déni de service de type `CHARGEN` pourra être détecté par l'utilisation de son port caractéristique (UDP 19).

Niveau applicatif

La journalisation au niveau applicatif apporte des informations complémentaires. En effet, en prenant le cas d'un serveur mandataire HTTP, il est possible d'enregistrer de nombreuses données relatives au flux telles que :

- le domaine ;
- l'URI ;
- le *user-agent* ;
- le *referer* ;
- le code retour HTTP.

A titre d'exemple, le CERT-FR a été amené à traiter un incident relatif à un code malveillant utilisant un *user-agent* caractéristique. Si ce champ du protocole HTTP est journalisé, il est alors possible, à l'aide de cet indicateur, de rechercher l'ensemble des domaines contactés par le logiciel malveillant dans les journaux des serveurs mandataires du système d'informations. Une analyse du *referer* (ou URI source) d'une requête HTTP permettra également de trouver le site Web ayant redirigé un visiteur vers un domaine malveillant et de vérifier si d'autres machines ont également été redirigées depuis ce site.

Le CERT-FR recommande ainsi de journaliser, de manière aussi exhaustive que possible, les champs applicatifs mis à disposition par les équipements et solutions. La problématique de la journalisation doit également faire l'objet d'une attention particulière lors de développements ou d'acquisitions de produits (finesse des journaux produits, format propriétaire binaire ou format ouvert standardisé, etc.).

Nous aborderons lors d'une prochaine publication la problématique de la conservation et de l'accessibilité des journaux.

Documentation

- Note sur la mise en œuvre d'un système de journalisation :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Journalisation_NoteTech.pdf

2 - Attribut de groupe primaire dans Active Directory

Le champ `PrimaryGroupID` fait partie des attributs obligatoires d'un objet Active Directory de type utilisateur ou ordinateur. Méconnu, ce champ est pourtant important en particulier vis-à-vis des droits accordés à un utilisateur. Cet article se propose de décrire son utilité et son fonctionnement ainsi que de proposer des recommandations associées.

Ce champ, de type numérique, contient le `RID` (« Relative IDentifier ») du groupe marqué comme primaire pour l'utilisateur ou l'ordinateur. Le groupe primaire est utilisé en particulier dans les programmes de type POSIX supportés dans certaines éditions de Windows.

Ainsi, parmi les différents groupes de domaine auquels appartient un utilisateur ou un ordinateur, un groupe est toujours marqué comme groupe primaire. L'identifiant de ce groupe est alors mis dans le champ `PrimaryGroupID` et l'utilisateur retiré du groupe.

Dans une configuration par défaut d'un Active Directory, le champ `PrimaryGroupID` est fixé aux valeurs suivantes :

- utilisateur intégré « administrateur » : groupe « Admins du domaine » (RID 512)
- tous les utilisateurs autres qu'Administrateur et Invité : groupe « Utilisateurs de domaine » (RID 513)
- utilisateur intégré « Invité » : groupe « Invités du domaine » (RID 514)
- toutes les machines autres que les contrôleurs de domaine : groupe « Ordinateurs du domaine » (RID 515)
- contrôleurs de domaine : groupe « Contrôleurs de domaine » (RID 516)

Afin que l'utilisateur bénéficie des droits accordés à son groupe primaire, l'identifiant de sécurité de ce groupe (SID domaine + RID groupe) est ajouté dans le contexte de sécurité de l'utilisateur lorsque celui-ci s'authentifie. Il est donc important de noter que lorsqu'un utilisateur bénéficie de l'appartenance à un groupe via son attribut `PrimaryGroupID`, il n'est techniquement pas membre du groupe concerné (le SID de l'utilisateur n'est pas présent dans l'attribut « members » du groupe). Ceci se manifeste notamment lors de l'énumération des membres d'un groupe à travers une requête LDAP.

Ainsi, dans une configuration Active Directory par défaut, tous les utilisateurs (hors Administrateur et Invité) ont leur attribut `PrimaryGroupID` fixé à 513 et possèdent l'identifiant du groupe « Utilisateurs de domaine » dans leur contexte de sécurité, alors que le groupe « Utilisateurs de domaine » est techniquement vide. Ce comportement pourrait être utilisé à des fins malveillantes, notamment afin de dissimuler l'appartenance à un groupe disposant de privilèges importants. Cependant, certains éditeurs de groupes, en particulier ceux de Microsoft, prennent en compte ce mécanisme et font virtuellement apparaître les membres dont l'appartenance est issue du champ `PrimaryGroupID`.

Le CERT-FR recommande :

- de ne modifier les valeurs par défaut des attributs `PrimaryGroupID` qu'en cas de nécessité applicative ;
- d'auditer régulièrement les valeurs du champ `PrimaryGroupID` de tous les utilisateurs et ordinateurs d'un domaine, afin d'identifier d'éventuelles dérives ;
- de repositionner la valeur par défaut du champ `PrimaryGroupID` si une modification injustifiée est constatée.

3 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié sept bulletins de sécurité, dont deux considérés comme critiques :

- MS14-030 (important) qui concerne le Bureau à distance de Microsoft Windows ;
- MS14-031 (important) qui concerne le protocole TCP de Microsoft Windows ;
- MS14-032 (important) qui concerne Microsoft Lync Server ;
- MS14-033 (important) qui concerne Microsoft XML Core Services ;
- MS14-034 (important) qui concerne Microsoft Word ;
- MS14-035 (critique) qui concerne Microsoft Internet Explorer ;
- MS14-036 (critique) qui concerne le composant Microsoft Graphics.

Ce mois-ci, Microsoft a corrigé 59 vulnérabilités concernant Internet Explorer. Deux d'entre elles étaient déjà connues publiquement :

- CVE-2014-1770 qui concerne une corruption de mémoire ;
- CVE-2014-1771 qui concerne la négociation des certificats au cours d'une session TLS.

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-261/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-262/index.html

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-263/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-264/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-265/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-266/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-267/index.html

4 - Rappel des avis émis

Dans la période du 06 au 12 juin 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-254 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2014-AVI-255 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2014-AVI-256 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-257 : Multiples vulnérabilités dans les produits Huawei
- CERTFR-2014-AVI-258 : Vulnérabilité dans Xen
- CERTFR-2014-AVI-259 : Multiples vulnérabilités dans EMC Documentum Digital Asset Manager
- CERTFR-2014-AVI-260 : Multiples vulnérabilités dans Blue Coat
- CERTFR-2014-AVI-261 : Vulnérabilité dans le Bureau à distance de Microsoft Windows
- CERTFR-2014-AVI-262 : Vulnérabilité dans le protocole TCP de Microsoft Windows
- CERTFR-2014-AVI-263 : Vulnérabilité dans Microsoft Lync Server
- CERTFR-2014-AVI-264 : Vulnérabilité dans Microsoft XML Core Services
- CERTFR-2014-AVI-265 : Vulnérabilité dans Microsoft Word
- CERTFR-2014-AVI-266 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-267 : Multiples vulnérabilités dans le composant Microsoft Graphics
- CERTFR-2014-AVI-268 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-269 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-270 : Multiples vulnérabilités dans les produits Mozilla

Gestion détaillée du document

13 juin 2014 version initiale.