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 12 septembre 2014
N° CERTFR-2014-ACT-037

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-037

1 - Déplacement latéral au sein d'un réseau Microsoft Windows (Première partie)

Cet article, en deux parties, vise à fournir aux spécialistes en investigation numérique des axes d'analyse pertinents pour identifier les traces d'un déplacement latéral au sein d'un environnement Microsoft Windows.

Lorsqu'une machine compromise est identifiée, l'équipe de réponse à incident doit analyser l'activité de l'attaquant sur le poste. Dans les attaques de grande ampleur, ce dernier a très fréquemment pour objectif d'étendre son emprise sur d'autres postes du réseau afin de prendre le contrôle du domaine ou plus simplement d'identifier les ressources les plus intéressantes.

Dans cette optique, il commence une phase de reconnaissance qui vise à collecter des données techniques utiles pour établir une cartographie du réseau et identifier les machines d'intérêt. Les recherches initiales concernent généralement la première machine compromise par l'attaquant (patient zéro de la compromission) : identification du système d'exploitation utilisé, configuration des interfaces du réseau, partages réseau utilisés/disponibles, services configurés, utilisateurs du poste, etc. Certaines applications présentes par défaut sur un système Windows permettent bien souvent à l'attaquant d'obtenir ces informations (`ipconfig`, `systeminfo`, `tasklist`, `net`, etc.). L'attaquant dresse également une cartographie du réseau accessible pour identifier les zones accessibles directement.

Par la suite, l'attaquant tente d'obtenir des couples identifiant / mot de passe pour augmenter son niveau de privilèges sur le poste ou sur le domaine. La méthode la plus fréquemment rencontrée concerne le vol d'un couple identifiant / mot de passe d'un administrateur local, voire d'un administrateur du domaine.

L'attaquant peut recourir à diverses techniques (découverte d'un mot de passe trivial, « *pass-the-hash* », exploitation d'une vulnérabilité, etc.) à l'aide d'outils largement diffusés sur Internet. Muni de ces informations, l'attaquant peut être dans la capacité de se connecter à un poste distant et de maintenir ses accès. Pour chaque machine d'intérêt, il recommencera le processus de collecte de données afin d'affiner progressivement sa vision de l'architecture réseau et obtenir le niveau de privilège adéquat.

Du point de vue de l'analyse, il convient donc de s'intéresser au trafic réseau généré par un système compromis. A ce titre, il est possible de caractériser rapidement un comportement suspect :

- balayage de ports sur des machines du réseau ;
- connexion RDP (Remote Desktop Protocol) entrante ou sortante (port 3389);
- connexion réseau avec des hôtes inhabituels, au sein du réseau ou à l'extérieur si le poste est accessible depuis Internet;
- connexion utilisant un protocole spécifique ou non identifié;
- volumétrie ou heures de connexion inhabituelles.

Pour détecter des comportements anormaux, l'analyste doit avoir une connaissance précise du réseau compromis (flux légitimes, fonctions des postes, filtrages existants, etc.). L'exploitation des traces issues du système est complexe, car l'attaquant a souvent recours à des fonctionnalités natives de Windows.

Il faut donc être en mesure de discriminer l'activité légitime du système et celle de l'attaquant. Les manipulations effectuées en ligne de commande, qui laissent moins de traces qu'une interaction avec l'explorateur Windows, peuvent être plus difficiles à exploiter par l'analyste.

Afin d'avoir une vision précise de l'activité de l'attaquant, l'investigateur devra impérativement croiser les informations extraites des différents systèmes compromis. L'établissement d'une chronologie globale est une méthode efficace pour donner du sens aux données découvertes. Une liste, non exhaustive, d'artefacts exploitables sur un poste Microsoft Windows est présentée ci-dessous.

L'analyste ne doit pas oublier qu'il peut également extraire ces données depuis les points de restauration créés disponibles sous Windows (XP : « RestorePoints », Vista et supérieur : « Volume Shadow Copies ») et remonter ainsi au plus près de la compromission du poste si nécessaire.

Identifier les programmes exécutés

L'examen de ces données vise à lister les programmes que l'attaquant a pu exécuter. L'analyste devra s'intéresser notamment aux programmes :

- liés à des fonctionnalités réseau : net.exe, net1.exe, ping.exe, netstat.exe, nbtstat.exe, nslookup.exe, ftp.exe, route.exe ;
- inconnus ou au nom aléatoire;
- exécutés dans un temps proche de la compromission initiale ;
- liés à des fonctionnalités système spécifiques :
  - tâches planifiées : at.exe, schtasks.exe,
  - services : sc.exe, tasklist.exe,
  - interpréteur de commandes : cmd.exe, powershell.exe ,
  - manipulation de la base de registre : reg.exe, regedit.exe, Regsvr32.exe ,
  - manipulation de fichiers : xcopy.exe, makecab.exe, winrar.exe ;
- de récupération de couples identifiants et mots de passe comme mimikatz, Pwdump, Windows Credential Editor (WCE), Lslsass ;
- d'exécution de code à distance : psexec.exe, psexesvc.exe, runas.exe ;
- lancé depuis un chemin inhabituel (dossier temporaire, dossier utilisateur) ;
- de prise de contrôle à distance tel UltraVNC, Logmein ;
- issus de la suite Sysinternals (PsLoggedOn, ShareEnum, PsInfo, etc.).

Ces données pourront être extraites des artefacts suivants :

- Prefetch : mécanisme utilisé pour accélérer le démarrage des applications. Les fichiers « *.pf » situés dans le dossier Prefetch permettent d'identifier des ressources nécessaires à l'application et des dates d'exécution (premier et dernier lancement). Emplacement : `c:\Windows\Prefetch`
- Bases de registre :
  - UserAssist : enregistrements liés à l'exécution de programmes par un utilisateur via l'explorateur Windows ("explorer.exe") contenant le nombre d'exécutions d'un programme et sa date de dernier lancement. Emplacement : "ntuser.dat" `\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`
  - MUI Cache : enregistrements liés à l'exécution de programmes par un utilisateur. Emplacement :
    - XP : "ntuser.dat" `\Software\Microsoft\Windows\ShellNoRoam\MUICache`
    - Vista et supérieur : "ntuser.dat" `\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache`
  - RunMRU : enregistrements liés à l'exécution d'une commande via le champ « Exécuter » du menu « Démarrer ». Emplacement : "ntuser.dat" `\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`
  - AppcompatCache : enregistrements liés à l'application de règles de compatibilité spécifiques en cas d'exécution d'un programme. Emplacement :
    - XP : "System" `ControlSetXX\Control\SessionManager\AppCompatibility\AppCompatCache`
    - Vista et supérieur : "System" `ControlSetXX\Control\SessionManager\AppCompatCache\AppCompatCache`

- Sysinternals - Acceptation de la licence. Clé de registre créée lors de l'acceptation de la licence d'utilisation de produits Sysinternals. Emplacement : "ntuser.dat"
  `\Software\Sysinternals`
- Journaux d'évènements : Les journaux d'évènements (notamment « Application », « System » et « Security ») peuvent contenir des informations liées à l'exécution d'une application. Par exemple le lancement du service `PSEXESVC` dans le journal « System » pourra être relevé. Les journaux générés par les antivirus et le gestionnaire des tâches planifiés (« Microsoft-Windows-TaskScheduler/Operational») peuvent également contenir des informations utiles. Emplacement :
  - XP : `C:\Windows\System32\config`
  - Vista et supérieur : `C:\Windows\System32\winevt\Logs`

2 - Mise à jour mensuelle de Microsoft

Le 09 septembre 2014, lors de sa mise à jour mensuelle, Microsoft a publié quatre bulletins de sécurité dont un considéré comme critique et trois comme importants :

- MS14-052 (critique) qui concerne Internet Explorer ;
- MS14-053 (important) qui concerne .NET ;
- MS14-054 (important) qui concerne le planificateur de tâches de Windows ;
- MS14-055 (important) qui concerne Lync Server.

Cette mise à jour corrige 37 vulnérabilités dans Internet Explorer. La plupart d'entre elles sont des corruptions de mémoires susceptibles de permettre une exécution de code arbitraire à distance. Une des vulnérabilités corrigées (CVE-2013-7331) était déjà connue publiquement et exploitée dans le cadre d'attaques ciblées.

La vulnérabilité corrigée dans .NET peut conduire à un déni de service pour un site Internet basé sur .NET si des requêtes spécifiques lui sont soumises.

Concernant Lync Server, trois vulnérabilités sont corrigées. Elles peuvent conduire à un déni de service ou à une fuite d'information si un utilisateur clique sur une URL spécialement conçue.

Enfin, la vulnérabilité affectant le planificateur de tâches de Windows permet une élévation locale de privilèges si un attaquant arrive à se connecter sur un système vulnérable et à exécuter un programme spécialement conçu.

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-375/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-376/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-377/index.html
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-AVI-378/index.html

3 - Rappel des avis émis

Dans la période du 05 au 11 septembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-374 : Vulnérabilité dans Cisco Unified Computing System
- CERTFR-2014-AVI-375 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-376 : Vulnérabilité dans Microsoft .NET
- CERTFR-2014-AVI-377 : Vulnérabilité dans Microsoft Windows
- CERTFR-2014-AVI-378 : Multiples vulnérabilités dans Microsoft Lync Server
- CERTFR-2014-AVI-379 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2014-AVI-380 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-381 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2014-AVI-382 : Multiples vulnérabilités dans VMware vSphere
- CERTFR-2014-AVI-383 : Vulnérabilité dans HP Network Node Manager I

Gestion détaillée du document

12 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-037