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 octobre 2015
N° CERTFR-2015-ACT-041

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-041

1 - WMI

Introduction

Le service de gestion Windows Management Instrumentation (WMI) est aujourd'hui largement utilisé par les administrateurs système, afin de gérer les infrastructures Windows dont ils ont la charge. Ces opérations sont réalisées localement ou à travers le réseau de l'entité.

Cependant, le CERT-FR observe une popularité grandissante de WMI parmi les acteurs offensifs. Certaines capacités de cette technologie sont ainsi particulièrement appréciées :

- la reconnaissance des systèmes ;
- la détection d'antivirus et de virtualisation ;
- l'exécution de code à distance ;
- le déplacement latéral au sein du réseau ;
- la persistance sur un système compromis ;
- l'exfiltration discrète d'informations.

De plus, ce service est démarré par défaut sur toutes les versions de Windows depuis Windows ME. Il est légitime et ne fait donc pas l'objet d'une suspicion par l'analyste forensique (ainsi que les IPS et autres anti-virus). Enfin, son utilisation laisse peu de traces. Dès lors, avec cette technologie, l'attaquant dispose d'un moyen discret et efficace pour compromettre un système.

L'intention de cet article est de fournir aux équipes de réponse aux incidents des éléments d'analyse pertinents pour identifier une compromission reposant sur WMI.

Architecture

Les informations du système sont collectées par le service WMI (winmgt), grâce au fournisseur (provider) implémenté sous la forme d'un composant COM (Component Object Model).

Un client WMI (powershell, wmic, winrm, etc) effectue une requête WQL (WMI SQL) pour récupérer les propriétés d'un objet (par exemple, on peut citer les objets de la classe win32_logicalDisk). Celle-ci est dirigée vers le fournisseur approprié (dans notre exemple, le provider en charge de la gestion des disques). Ce dernier va alors construire la liste des résultats (DevideID, DriveType, etc..) et les renvoyer au client via le service WMI :

```
Get-wmiObject win32_logicaldisk    <= classe win32_logicaldisk

DeviceID : C:    <= instance #1 de la classe win32_logicaldisk
DriveType : 3
ProviderName :
FreeSpace : 41835704320
Size : 319802044416
VolumeName : Windows
```

```
DeviceID : D:    <= instance #2 de la classe win32_logicaldisk
DriveType : 5
ProviderName :
FreeSpace :
Size :
VolumeName :
```

Protocole d'accès à distance

Afin de collecter ces données à distance, Microsoft propose 2 protocoles :

- Distributed component Object Model (DCOM) ;
- Windows Remote Management (WinRM).

WinRM n'est pas activé par défaut, mais peut l'être en utilisant wmi. Du point de vue de l'attaquant, ces deux protocoles sont intéressants puisque leurs flux sont rarement inspectés avec le même niveau d'expertise que les flux « Internet », comme HTTP, DNS, etc. Le protocole DCOM, basé sur MS-RPC, établit une connexion TCP initiale sur le port TCP 135 (RPC Endpoint Mapper). Les données sont ensuite échangées sur un port éphémère attribué dynamiquement. Le service WinRM, quant à lui, écoute sur le port TCP 5985 (HTTP) ou TCP 5986 (HTTPS) pour échanger des messages SOAP.

Effectuer une action avec WMI

Il existe plusieurs possibilités pour effectuer une action sur un poste à l'aide de WMI.

Avec les méthodes WMI

WMI permet d'accéder à la plupart des éléments de la configuration du poste (système de fichiers, base de registre, configuration des services). Une requête peut alors modifier une clé de registre tel que RestrictAnonymous, LAN Manager ou NullSessionShares:

```
Invoke-WmiMethod -computerName $Name -namespace Root\Default
   -class stdRegProv -Name SetString value
   -argumentList $hklm $key $data $value
```

Avec une exécution de code arbitraire

Une méthode communément utilisée par les attaquants est la méthode Create, de la classe Win32_process. Celle-ci permet de créer un nouveau processus localement ou sur une machine distante.

```
Invoke-WmiMethod -class win32_process -Name Create
   -ArgumentList "malicious.exe" -ComputerName WIN81
   -Credential "winlab\Administrator"
```

En utilisant les filtres d'évènements

WMI permet la création de filtres sur un évènement particulier (sous la forme d'une requête WQL), qui sera exécuté de façon régulière sur le système.

Par exemple, une requête peut être utilisée pour identifier les évènements suivants :

- création d'un processus particulier ;
- chargement d'une dll dans un processus ;
- insertion d'un média amovible ;
- création, modification ou destruction d'un fichier dans un répertoire.

Une fois le filtre configuré, il est utilisé pour déclencher l'action préconfigurée (event consumer). Parmi ces actions :

- LogFileEventConsumer : Écrit le contenu de l'évènement dans un log spécifique ;
- CommandLineEventConsumer : Exécute une ligne de commande arbitraire (avec les droits System) ;
- ActiveScriptEventConsummer : Exécute un script VBscript.

Certaines plateformes de test de pénétration basées sur Powershell enregistrent un filtre permanent sur un évènement, comme le démarrage du système, et y associent une action du type CommandLineEventConsumer.

Celle-ci exécutera les commandes powershell configurées en argument sans qu'il soit nécessaire de créer un fichier sur la machine compromise. Cette technique a bien-sûr pour objectif de tromper l'analyste forensique trop habitué à se concentrer sur les artefacts liés au système de fichiers (ou la base de registre).

L'utilisation de filtre permanent peut être détournée par l'attaquant souhaitant n'exécuter qu'une seule fois son action malveillante. Pour cela, il lui suffit de configurer l'event consumer pour effacer ses traces (le filtre d'évènement, le consumer et le binding).

Mode de stockage furtif

La possibilité de créer ses propres classes WMI, localement ou à distance, permet à un attaquant de stocker puis d'exfiltrer des données à distance [Andrei Dumitrescu]. Il détourne ainsi son usage habituel pour en faire un canal de contrôle.

« Push attack » : L'attaquant crée à distance une classe « Win32_EvilClass » contenant des propriétés «EvilProperty», dans laquelle il peut exfiltrer d'une machine A vers une machine B les données de son choix.

« Pull attack » : Par exemple, l'attaquant crée une clé de registre « EvilKey » dans laquelle il stocke les résultats des commandes préalablement exécutées (par exemple Get-Process lsass). Le résultat de la commande peut donc ensuite aisément (et discrètement) être récupéré à distance.

Bien sûr, l'attaquant peut aussi combiner ces deux techniques pour éviter toute utilisation d'un moyen de stockage ou de communication habituellement monitoré sur les réseaux d'entreprise. Enfin, l'installation d'un provider malveillant permet à l'attaquant de conserver un accès à distance sur le poste compromis.

Défense

La gestion des ressources Windows est aujourd'hui souvent dépendante de ce service. Le choix de désactiver cette fonctionnalité ne doit être pris sans avoir préalablement réalisé une étude d'impact.

Une mesure intermédiaire peut consister à bloquer les flux WMI afin d'empêcher l'exécution de WMI à distance. Il suffit de configurer WMI pour utiliser un port fixe [WMI port] afin de pouvoir le bloquer au niveau approprié (sous-réseau, DMZ, etc).

Journalisation

Les journaux suivants enregistrent les évènements liés à WMI :

- Microsoft-Windows-WinRM/Operational: indique les connexions WinRM ;
- Microsoft-Windows-DistributedCOM : indique les connexions DCOM ;
- Microsoft-Windows-WMI-Activity/Operational : indique les requêtes WMI effectuées ainsi que les méthodes appelées. Il permet donc à l'analyste d'identifier des activités potentiellement malveillantes.

Par ailleurs, il convient d'activer la stratégie d'audit de création de processus afin d'inclure les informations sur les commandes transmises à chaque processus (Event id 4688) [command line auditing]. Attention à l'impact sur les journaux, augmenter la taille et éventuellement réserver ces configurations à des machines sensibles (DCs, etc.).

Pour mettre en évidence l'usage malveillant de filtres d'évènement, l'outil Autoruns de Sysinternals permet de les visualiser.

On pourra aussi utiliser les commandes PowerShell suivantes :

```
Get-WMIObject -Namespace root\Subscription -Class __EventFilter
Get-WMIObject -Namespace root\Subscription -Class __EventConsumer
Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding
```

Références

- WMI port - Setting Up a Fixed Port for WMI :
  https://msdn.microsoft.com/en-us/library/bb219447%28v=vs.85%29.aspx
- command line auditing :
  https://technet.microsoft.com/en-us/library/dn535776.aspx
- Windows Logging Cheat+Sheet :
  http://malwarearchaeology.squarespace.com/cheat-sheets

2 - Vulnérabilités dans le pilote de TrueCrypt

De multiples vulnérabilités affectant le pilote du logiciel de chiffrement de disque "TrueCrypt" ont été découvertes par James Forshaw, membre de l'équipe de recherche "Google Project Zero".

Ces vulnérabilités affectent le pilote "truecrypt.sys" embarqué dans l'installeur de TrueCrypt. Ce logiciel n'étant plus maintenu, les vulnérabilités ne seront pas corrigées.

Ces bogues affectent également des logiciels dérivés tels que CipherShed et VeraCrypt. Ce dernier est toujours maintenu et corrige ces problèmes de sécurité depuis la version 1.15.

Le chercheur a identifié deux vulnérabilités pouvant amener à une élévation de privilèges. La première permettrait à un utilisateur de manipuler les volumes chiffrés montés par d'autre utilisateur sur la même machine, tandis que la seconde permettrait de monter un volume chiffré en utilisant une lettre de disque existante.

Analyse de la vulnérabilité CVE-2015-7358

Lors du montage d'un volume chiffré dans TrueCrypt, le pilote va tenter de créer la lettre du disque demandé en appelant la function IoCreateSymbolicLink(). Pour éviter la redéfinition d'une lettre existante, un appel est fait à la fonction "IsDriverLetterAvailable()", qui va tenter de lire le lien symbolique « \DosDevices\X: » via la function ZwOpenSymbolicLinkObject(). Elle renvoie FALSE si le lien a été correctement ouvert ou TRUE dans le cas échéant.

C'est dans cette fonction que se situe le dysfonctionnement.

```
if (NT_SUCCESS(ZwOpenSymbolicLinkObject(&handle, GENERIC_READ,
            &objectAttributes))) {
    ZwClose(handle);
    return FALSE;
}
return TRUE;
```

Le problème vient de la macro NT_SUCCESS. Cette macro renvoie TRUE si la valeur de retour de la fonction est comprise entre 0-0x3FFFFFFF ou entre 0x40000000-0x7FFFFFFF.

Les valeurs de retour correspondant à la plage des erreurs sont comprises entre 0xC0000001 (STATUS_UNSUCCESSFUL) et 0xC01A002E (STATUS_LOG_INCONSISTENT_SECURITY) : si ZwOpenSymbolicLinkObject() renvoie une erreur (quelque soit l'erreur), la fonction IsDriverLetterAvailable() renverra TRUE.

Si un autre type d'objet est crée avec le même nom que le lien symbolique, la fonction renverra l'erreur STATUS_OBJECT_TYPE_MISMATCH. Il sera ensuite possible de supprimer le lien symbolique d'origine (« \DosDevices\C: » si on veut remplacer le lien « C: » par exemple) et de le remplacer par un lien pointant vers le volume TrueCrypt.

Une exploitation possible de cette vulnérabilité pourrait être de recréer une arborescence \%windir%\System32 dans un conteneur TrueCrypt et d'y placer un binaire qui aura le même nom qu'un binaire lancé avec des droits privilégiés par le système. Par exemple, lorsque la combinaison Ctrl+Alt+Suppr est exécuté, "dllhost.exe" est exécuté avec les droits SYSTEM.

Si la vulnérabilité est exploitée pour lier le volume TrueCrypt à la lettre du disque C: et que Ctrl+Alt+Suppr est exécuté, alors le binaire "dllhost.exe" de l'attaquant sera exécuté.

Recommandations

Le CERT-FR recommande d'utiliser des logiciels pouvant bénéficier de correctifs de sécurité de la part de leur éditeur. De plus, le CERT-FR recommande d'utiliser des produits certifiés par l'ANSSI.

Documentation

- Détails sur la vulnérabilité :
  https://code.google.com/p/google-security-research/issues/detail?id=538
- Alerte CERTFR-2015-AVI-420 du 8 octobre 2015 :
  http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-420/
- Produits certifiés par l'ANSSI :
  http://www.ssi.gouv.fr/administration/produits-certifies/

3 - Rappel des avis émis

Dans la période du 05 au 11 octobre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-417 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2015-AVI-418 : Multiples vulnérabilités dans Google Nexus
- CERTFR-2015-AVI-419 : Vulnérabilité dans le noyaux Linux d'Ubuntu
- CERTFR-2015-AVI-420 : Multiples vulnérabilités dans Veracrypt

Durant la même période, les publications suivantes ont été mises à jour :

- CERTFR-2015-ALE-010-001 : Multiples vulnérabilités dans Google Android (fermeture de l'alerte.)

Gestion détaillée du document

12 octobre 2015 version initiale.