RootkitRevealer v1.71

Introduction

RootkitRevealer est un utilitaire de détection de rootkit avancé. Il s'exécute sur Windows NT 4 et versions supérieures et sa fenêtre de résultats affiche les incohérences de l'API du Registre et du système de fichiers qui peuvent indiquer la présence d'un rootkit en mode utilisateur ou en mode noyau. RootkitRevealer détecte tous les rootkits persistants, notamment AFX, Vanquish et HackerDefender (remarque : RootkitRevealer ne détecte pas les rootkits tels que Fu qui n'essaient pas de dissimuler leurs fichiers ou leurs clés de Registre). Si vous l'utilisez pour identifier la présence d'un rootkit, merci de nous le faire savoir !

La raison pour laquelle il n'existe plus de version de ligne de commande est que les auteurs de logiciels malveillants ont commencé à cibler la détection de RootkitRevealer en utilisant son nom exécutable. Par conséquent, nous avons mis à jour RootkitRevealer pour lui permettre d'effectuer son analyse à partir d'une copie de lui-même portant un nom aléatoire et s'exécutant en tant que service Windows. Ce type d'exécution n'est pas compatible avec une interface de ligne de commande. Notez que vous pouvez utiliser les options de ligne de commande pour exécuter une analyse automatique avec les résultats enregistrés sur un fichier, ce qui équivaut au comportement de la version de ligne de commande.

Haut de page

Qu'est qu'un rootkit

Le terme rootkit décrit les mécanismes et techniques utilisés par les logiciels malveillants, notamment les virus, les logiciels espions et les chevaux de Troie, pour essayer de se dissimuler et d'éviter d'être détectés par les outils de blocage de logiciels espions, les antivirus et les utilitaires de gestion de système. Il existe plusieurs classifications des rootkits, selon que les logiciels malveillants survivent aux procédures de redémarrage ou qu'ils s'exécutent en mode utilisateur ou en mode noyau.

Rootkits persistants

Un rootkit persistant est associé aux logiciels malveillants qui s'activent à chaque démarrage du système. Vu que ces logiciels malveillants contiennent du code qui doit être automatiquement exécuté à chaque démarrage du système ou lorsqu'un utilisateur se connecte, ils doivent enregistrer ce code dans un magasin persistant, tel que le Registre ou le système de fichiers, et configurer une méthode permettant au code de s'exécuter sans l'intervention de l'utilisateur.

Rootkits basés sur la mémoire

Les rootkits basés sur la mémoire sont des logiciels malveillants qui n'ont pas de code persistant et ne survivent donc pas à un redémarrage.

Rootkits en mode utilisateur

Les rootkits utilisent un grand nombre de moyens pour essayer d'échapper à la détection. Par exemple, un rootkit en mode utilisateur pourrait intercepter tous les appels aux API FindFirstFile/FindNextFile de Windows qui sont utilisées par les utilitaires d'exploration de système de fichiers, y compris Explorer et l'invite de commande, afin d'énumérer le contenu des répertoires de système de fichiers. Lorsqu'une application exécute une liste d'annuaires qui, autrement, renverrait des résultats contenant des entrées identifiant les fichiers associés au rootkit, le rootkit intercepte et modifie les résultats pour supprimer

les entrées.

L'API native de Windows sert d'interface entre les clients en mode utilisateur et les services en mode noyau, et les rootkits en mode utilisateur plus sophistiqués interceptent le système de fichiers, le Registre et les fonctions d'énumération de processus de l'API native. Ceci empêche leur détection par les analyseurs qui comparent les résultats d'une énumération d'une API Windows avec les résultats renvoyés par une énumération d'une API native.

Rootkits en mode noyau
Les rootkits en mode noyau peuvent être encore plus puissants puisqu'ils peuvent non seulement intercepter l'API native en mode noyau, mais également manipuler directement les structures de données en mode noyau. L'une des techniques courantes pour masquer la présence d'un processus de logiciel malveillant consiste à supprimer le processus de la liste des processus actifs du noyau. Dans la mesure où les API de gestion de processus comptent sur le contenu de la liste, le processus de logiciel malveillant n'affichera pas les outils de gestion intraprocessus tels que le Gestionnaire des tâches ou Process Explorer.

Haut de page

Fonctionnement de RootkitRevealer

Puisque les rootkits persistants modifient les résultats d'API de sorte qu'une vue système utilisant des API diffère de la véritable vue du stockage, RootkitRevealer compare les résultats d'une analyse système au plus haut niveau à ceux d'une analyse au plus bas niveau. Le plus haut niveau est l'API de Windows et le plus bas niveau est le contenu brut d'un volume de système de fichiers ou d'une ruche du Registre (un fichier ruche est le format de stockage sur disque du Registre). Par conséquent, les rootkits en

mode utilisateur ou noyau qui manipulent l'API de Windows ou l'API native pour supprimer leur présence d'une liste de répertoire, par exemple, seront considérés par RootkitRevealer comme une incohérence entre les informations renvoyées par l'API de Windows et celles qui sont détectées lors de l'analyse brute des structures du système de fichiers du volume FAT ou NTFS.

Un rootkit peut-il éviter d'être détecté par RootkitRevealer ?
Théoriquement, un rootkit peut éviter d'être détecté par RootkitRevealer. Pour ce faire, il doit intercepter les lectures des données de ruche du Registre ou des données du système de fichiers de RootkitRevealer et modifier le contenu des données de sorte que les données ou fichiers du Registre du rootkit ne soient pas présents. Cependant, ceci nécessiterait un niveau de sophistication qui n'a pas été atteint à ce jour. Les modifications des données nécessiteraient une connaissance extrêmement approfondie des formats NTFS et FAT et des formats de ruche du Registre, ainsi que la possibilité de changer les structures de données de sorte qu'elles masquent le rootkit sans créer de structures incohérentes ou non valides, ou d'incohérences secondaires qui seraient indiquées par RootkitRevealer.

Existe t-il un moyen incontournable de détecter la présence d'un rootkit ?
De façon générale, pas à partir d'un système en cours d'exécution. Un rootkit en mode noyau peut contrôler n'importe quel aspect du comportement d'un système et compromettre ainsi les informations renvoyées par une API, y compris les lectures brutes des ruches du Registre et des données du système de fichiers effectuées par RootkitRevealer. La comparaison d'une analyse en ligne d'un système et d'une analyse hors ligne d'un environnement sécurisé tel qu'un démarrage dans une installation CD de système d'exploitation est certes plus fiable, mais les rootkits peuvent cibler de tels outils et échapper à leur détection.

Il n'y existera probablement jamais d'analyseur de rootkits universel, mais les analyseurs les plus puissants seront les analyseurs de comparaison en ligne ou hors ligne qui s'intègrent aux antivirus.

Haut de page

Utilisation de RootkitRevealer

Le compte à partir duquel RootkitRevealer est exécuté doit disposer de privilèges de sauvegarde de fichiers et répertoires, de chargement de pilotes et d'exécution de tâches de maintenance de volume (sur Windows XP et supérieur). Par défaut, c'est le groupe Administrateurs qui dispose de ces privilèges. Afin de minimiser les faux positifs, exécutez RootkitRevealer sur un système inactif.

Pour un résultat optimal, fermez toutes les applications et laissez le système inactif pendant le processus d'analyse de RootkitRevealer.

Si vous avez des questions ou des problèmes, visitez le forum RootkitRevealer de Sysinternals.

Haut de page

Analyse manuelle

Pour analyser un système, lancez-le et appuyez sur le bouton Scan. RootkitRevealer analyse le système et signale ses actions dans une zone d'état au bas de sa fenêtre tout en notant les incohérences dans la liste des résultats. Options configurables :

- **Hide NTFS Metadata Files :** Cette option est activée par défaut, et RootkitRevealer n'affiche pas les fichiers de métadonnées NTFS standard, qui sont masqués de l'API de Windows.
- **Scan Registry :** Cette option est activée par défaut. Si vous la désélectionnez, RootkitRevealer n'exécute pas d'analyse du Registre.

Haut de page

Lancement d'une analyse automatique

RootkitRevealer prend en charge plusieurs options d'analyse automatique des systèmes :

utilisation : rootkitrevealer [-a [-c] [-m] [-r] fichier de résultats]

-a

Analyse automatiquement et quitte une fois l'analyse terminée.

-c

Formate les résultats en CSV

-m

Affiche les fichiers de métadonnées NTFS

-r

Ignore le Registre.

Notez que l'emplacement du fichier de résultats doit se trouver sur un volume local.

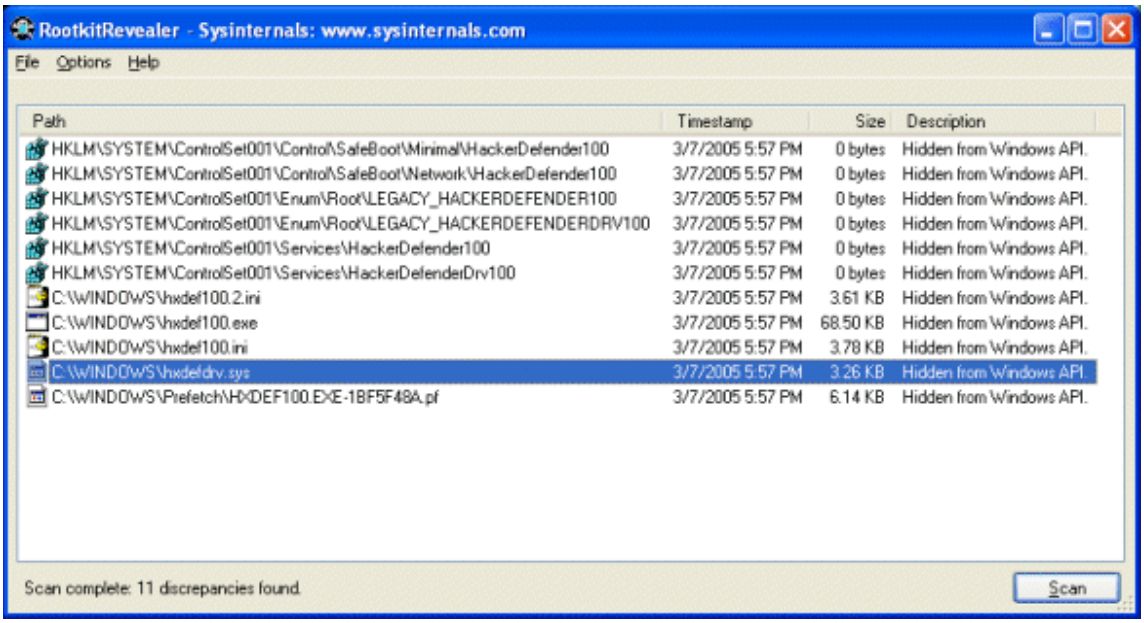
Si vous spécifiez l'option -c, Rootkitrevealer ne signale pas la progression et les incohérences sont imprimées au format CSV de façon à pouvoir être aisément importées dans une base de données. Vous pouvez exécuter des analyses de systèmes distants en les exécutant avec l'utilitaire PsExec de Sysinternals et en utilisant une ligne de commande comme suit :

psexec \\remote -c rootkitrevealer.exe -a c:\windows\system32\rootkit.log

Haut de page

Interprétation du résultat

Ceci est une capture d'écran de RootkitRevealer détectant la présence du rootkit HackerDefender. Les incohérences de la clé de Registre indiquent que les clés de Registre renfermant le pilote de périphérique et les paramètres de service de HackerDefender ne sont pas visibles par l'API de Windows mais sont présents dans l'analyse brute des données de ruche du Registre. De même, les fichiers associés à HackerDefender ne sont pas visibles par les analyses du répertoire de l'API de Windows mais sont présents dans l'analyse des données de système de fichiers brutes.



Vous devriez examiner toutes les incohérences et déterminer la probabilité qu'elles indiquent la présence d'un rootkit. Malheureusement, il n'existe pas de méthode entièrement fiable pour déterminer la présence d'un rootkit en fonction du résultat, mais vous devriez examiner toutes les incohérences signalées pour vous assurer qu'elles peuvent être expliquées. Si vous savez qu'un rootkit est installé sur votre système, recherchez des instructions sur le Web pour essayer de le supprimer. Si vous ne savez pas exactement comment supprimer un rootkit, vous devriez reformater le disque dur du système et réinstaller Windows.

En plus des informations sur les incohérences de RootkitRevealer ci-dessous, le forum RootkitRevealer de Sysinternals aborde les rootkits détectés et les faux positifs spécifiques.

Haut de page

Hidden from Windows API.

Ces incohérences sont celles que manifestent la plupart des rootkits ; cependant, si vous n'avez pas coché l'option Hide NTFS

metadata files, vous devez vous attendre à voir plusieurs de ces entrées sur le volume NTFS puisque NTFS masque ses fichiers de métadonnées tels que $MFT et $Secure de l'API de Windows. Les fichiers de métadonnées présents sur les volumes NTFS varient suivant la version de NTFS et les fonctionnalités de NTFS qui ont été activées sur le volume. Il existe également des produits antivirus, tels que Kaspersky Antivirus, qui utilisent des techniques de rootkit pour dissimuler les données qu'ils enregistrent dans les flux de données alternatifs de NTFS. Si vous exécutez un analyseur de virus de ce type, vous verrez une incohérence Hidden from Windows API pour un flux de données alternatif sur chaque fichier NTFS. RootkitRevealer ne prend pas en charge les filtres de résultat parce que les rootkits peuvent tirer avantage de n'importe quel système de filtrage. Enfin, vous pouvez également voir cette incohérence si un fichier est supprimé lors d'une analyse.

Voici la liste des fichiers de métadonnées NTFS définis à partir de Windows Server 2003 :

- $AttrDef
- $BadClus
- $BadClus:$Bad
- $BitMap
- $Boot
- $LogFile
- $Mft
- $MftMirr
- $Secure
- $UpCase

- $Volume
- $Extend
- $Extend\$Reparse
- $Extend\$ObjId
- $Extend\$UsnJrnl
- $Extend\$UsnJrnl:$Max
- $Extend\$Quota

Access is Denied.

RootkitRevealer ne devrait jamais signaler cette incohérence puisqu'il utilise des mécanismes qui lui permettent d'accéder à n'importe quel fichier, répertoire ou clé de Registre d'un système.

Visible in Windows API, directory index, but not in MFT.
Visible in Windows API, but not in MFT or directory index.
Visible in Windows API, MFT, but not in directory index.
Visible in directory index, but not Windows API or MFT.

Une analyse de système de fichiers est constituée de trois composants : l'API de Windows, le MFT (Master File Table) de NTFS et les structures d'index du Répertoire sur disque de NTFS. Ces incohérences indiquent qu'un fichier apparaît seulement dans une ou deux des analyses. Ceci est généralement dû au fait qu'un fichier est créé ou supprimé pendant les analyses. Voici un exemple de rapport d'incohérence de RootkitRevealer concernant un fichier créé pendant l'analyse :

C:\newfile.txt
01/03/05 17:26
8 bytes

Visible in Windows API, but not in MFT or directory index.

Windows API length not consistent with raw hive data.

Les rootkits peuvent tenter de se cacher en déformant la taille d'une valeur du Registre de sorte que son contenu ne soit pas visible par l'API de Windows. Vous devriez examiner de telles incohérences, bien qu'elles puissent également apparaître à la suite d'une modification des valeurs du Registre durant une analyse.

Type mismatch between Windows API and raw hive data.

Les valeurs du Registre ont un type, tel que DWORD et REG_SZ, et cette incohérence indique que le type d'une valeur tel que signalé par l'API de Windows diffère de celui des données de ruche brutes. Un rootkit peut masquer ses données en l'enregistrant en tant que valeur REG_BINARY, par exemple, et en faisant croire à l'API de Windows qu'il s'agit d'une valeur REG_SZ. Si elle est enregistrée en tant que 0 au démarrage des données, l'API de Windows ne pourra pas accéder à d'autres données.

Key name contains embedded nulls.

L'API de Windows traite les noms de clés comme des chaînes terminées par null tandis que le noyau les traite comme des chaînes comptées. Ainsi, il est possible de créer des clés de registre qui sont visibles par le système d'exploitation, mais seulement partiellement visibles par les outils du Registre tels que Regedit. L'exemple de code Reghide sur le site de Sysinternals démontre cette technique, qui est utilisée par les logiciels malveillants et les rootkits pour dissimuler les données du Registre. Utilisez l'utilitaire Regdellnull de Sysinternals pour

supprimer les clés comportant des nulls intégrés.

Data mismatch between Windows API and raw hive data.

Cette incohérence survient si une valeur du Registre est mise à jour durant l'analyse du Registre. Les valeurs qui changent fréquemment incluent les horodateurs tels que la valeur du temps de disponibilité de Microsoft SQL Server, indiquée ci-dessous, et les valeurs de la « dernière analyse » de l'analyseur de virus. Vous devrez examiner soigneusement toute valeur signalée pour vous assurer qu'il s'agit d'une application ou d'une valeur du Registre système valide.

HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\RECOVERYMANAGER\MSSQLServer\uptime_time_utc
01/03/05 16:33
8 bytes

Haut de page

Ressources sur les rootkits

Les sites Web et les documents suivants proposent plus d'informations sur les rootkits :

Comprendre les logiciels malveillants : Virus, logiciels espions et rootkits
Le webinaire Microsoft TechEd 2005 de Marc couvre les virus, les logiciels espions et les rootkits.

Sony, Rootkits and Digital Rights Management Gone Too Far
Consultez l'entrée de blog de Marc sur sa découverte et son analyse d'un rootkit de Sony sur un de ses ordinateurs.

Dénicher les rootkits
L'article du magazine Windows IT Pro de Marc propose un aperçu général de technologies des rootkits et se penche sur le fonctionnement de RootkitRevealer.

http://www.rootkit.nl/projects/rootkit_hunter.html
Ce site contient des exemples de code pour un certain nombre de rootkits en mode utilisateur et noyau ainsi que des discussions sur la façon de développer des rootkits.

Rootkits : Subverting the Windows Kernel
Ce livre de Greg Hoglund et Jamie Butler est l'analyse la plus complète des rootkits qui soit disponible.

www.phrack.org
Ce site enregistre les archives de Phrack, un magazine destiné aux « craqueurs » où les développeurs abordent les failles des produits de sécurité, les techniques de rootkits et d'autres pièges de logiciels malveillants.

research.microsoft.com/rootkit/
Page d'accueil sur les rootkits de Microsoft Research où Microsoft publie des livres blancs et des informations sur ses efforts visant à combattre les rootkits.

The Art of Computer Virus Research and Defense, de Peter Szor

Logiciels malveillants : Fighting Malicious Code, d'Ed Skoudis et Lenny Zeltser

Windows Internals, 4th Edition, de Mark Russinovich et Dave Solomon (ce livre n'aborde pas les rootkits, mais la connaissance de l'architecture de Windows aide à comprendre le fonctionnement des rootkits).