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 30 mai 2014
N° CERTFR-2014-ACT-022

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-022

1 - Prise de connaissance de l'environnement d'un poste à analyser

Ce bulletin d'actualité fait partie d'une série d'articles traitant de l'investigation numérique d'un système Microsoft Windows. L'objectif de ces articles est de présenter plusieurs bonnes pratiques d'analyse, d'identifier les artefacts à rechercher ou encore de décrire des cas rencontrés par le CERT-FR. Il s'agira d'effectuer un focus sur des thèmes particuliers et utiles lors d'une investigation numérique s'inscrivant dans une méthodologie de traitement d'incident (détection, préservation des données techniques, analyse, reconstruction). En effet, contrairement à la majorité des documentations qu'il est possible de retrouver sur Internet, l'investigation numérique telle qu'employée par le CERT-FR vise à détecter ou analyser un système compromis (périmètre de la compromission, mode opératoire de l'attaque, mécanisme de persistance, etc.) et non pas à rechercher un type de fichier spécifique (document classifié, image pédopornographique, etc.) Le sujet étant très vaste, les articles ne peuvent être complètement exhaustifs : les sujets abordés seront donc rédigés de manière synthétique en omettant volontairement certains détails techniques.

Il est rappelé qu'avant toute investigation numérique suite à détection d'une compromission, il est recommandé d'appliquer les bonnes pratiques détaillées sur la page Web du CERT-FR intitulée «Que faire en cas d'intusion ?» et notamment de veiller à la préservation les traces.

Le sujet traité ici consiste à présenter les paramètres techniques à extraire sur un système Windows (Windows XP, 7, 8 et 8.1) lors de la prise de connaissance de l'environnement technique.

Cette prise de connaissance pour une machine Windows potentiellement compromise est indispensable avant de mener une investigation numérique approfondie. Les éléments nécessaires sont principalement stockés au sein de la base de registre, dont les fichiers principaux sont situés dans le répertoire `Windows\system32\config` et dans les profils des utilisateurs.

La prise de connaissance consiste au minimum à identifier :

- la dernière configuration de la ruche `SYSTEM` : l'extraction des clés de la ruche `SYSTEM` de la base de registre (exemple : `SYSTEM\ControlSet002\services\vwifibus`) nécessite de connaître la valeur du paramètre `ControlSetX`, correspondant à `CurrentControlSet` sur une machine démarrée. Cette valeur est stockée sous le nom `Current` dans la clé `Select` de la ruche `SYSTEM`, et vaut par exemple 2 pour `ControlSet002` ;
- le nom de la machine (il convient de s'assurer que la machine est bien celle qu'il était prévu d'analyser) : la valeur `ComputerName` de la clé `ControlSetX\Control\ComputerName\ActiveComputerName` de la ruche `SYSTEM` fournit cette information (on pourra la confirmer en utilisant les valeurs `HostName` et `Domain` de la clé `HKLM\SYSTEM\ControlSetX\Services\Tcpip\Parameters`) ;
- la version exacte du système d'exploitation : cette information est indispensable dans la recherche automatique ou manuelle des artefacts. Elle est fournie à travers les valeurs de la clé `CurrentVersion` de la ruche `SOFTWARE` :
  - `Microsoft\Windows NT\CurrentVersion`
  - `Wow6432Node\Microsoft\Windows NT\CurrentVersion` (sous 64 bits uniquement)

- la date d'installation du système : cette information pourrait être par exemple corrélée avec la date de mise à disposition des souches système (masters) dans le but de réaliser une analyse différentielle. La valeur `InstallDate` de la clé `Microsoft\Windows NT\CurrentVersion` de la ruche `SOFTWARE` fournit cette information (heure en UTC). Attention, cette valeur doit être ignorée dans le cas des masters déployés en entreprise, car elle peut ne pas représenter la date de mise à disposition du poste à l'utilisateur, mais plutôt la date de création du master ;
- la dernière date d'extinction : cette date permet généralement de s'assurer que la machine n'était effectivement plus fonctionnelle à un instant donné. Elle est stockée dans la ruche `SYSTEM` sous la valeur `ShutdownTime` de la clé `ControlSetX\Control\Windows` (heure en UTC) ;
- la date de dernière écriture sur le disque : ce paramètre est redondant avec l'artefact précédent, il permet cependant de gérer le cas où la machine n'a pas été éteinte normalement. La recherche des dernières dates d'écriture stockées au sein de la MFT (Master File Table NTFS) permet généralement d'en avoir une bonne approximation ;
- le fuseau horaire : ce paramètre est indispensable pour corréler les dates issues de la machine avec d'autres événements ou journaux extérieurs (serveurs, serveur mandataire, etc.), cette information est stockée au sein de la clé `ControlSetX\Control\TimeZoneInformation` de la ruche SYSTEM. Beaucoup d'analyses sont faites en s'appuyant sur les dates. En général, les machines jointes à un domaine ont un référentiel de date fiable, en revanche, les machines sur des réseaux déconnectés et/ou en workgroup peuvent parfois présenter un écart de temps important. L'investigateur doit donc s'assurer de la date du système avant de l'éteindre pour collecter les traces et indices. On pourra aussi valider la configuration du service `w32time` pour s'assurer d'une synchronisation régulière avec un serveur de temps ;
- la dernière adresse IP utilisée sur chaque interface : ce paramètre est généralement utilisé pour corréler l'activité de la machine avec les événements issus d'équipements de filtrage ou de routage. Cette information est stockée sous `ControlSetX\Services\Tcpip\Parameters\Interfaces\ID_INTERFACE` dans la ruche `SYSTEM`;
- les utilisateurs et les dernières dates d'accès : le nom des utilisateurs locaux et de domaine ayant créé un environnement sur la machine (suite à une authentification interactive par exemple) est stocké au sein des clés `Microsoft\Windows NT\CurrentVersion\ProfileList\<SID utilisateur>` de la ruche `SOFTWARE`. La liste complète des utilisateurs locaux accompagnés d'informations d'authentification et d'historique est stockée dans plusieurs sous-clefs de la clef `SAM\Domains\Account\Users` de la ruche `SAM` (heures en UTC) ;
- la date des dernières mises à jour Windows : cela peut s'avérer pertinent dans les cas où la compromission d'une machine a été possible via une faille de sécurité. Ce paramètre ne permet pas de s'assurer que la machine soit à jour, mais peut prouver dans certains cas qu'elle ne l'était pas. La valeur `LastSuccessTime` de `Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\Results\Install` dans la ruche `SOFTWARE` donne cette information (heure en UTC) ;
- les voisinages réseau sur lesquels la machine a été connectée : on les trouve sous `Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache\Intranet` dans ruche `SOFTWARE` ;
- les points d'accès WiFi sur lesquels la machine s'est connectée. Cette information peut également servir à identifier les exfiltrations de données réalisées par le biais de points d'accès WiFi. On les retrouve dans ruche `SOFTWARE` sous `Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles`.

La majorité de ces artefacts peuvent être extraits automatiquement avec l'aide d'outils comme `RegRipper`.

Documentation

- RegRipper :
  https://code.google.com/p/regripper/
- Système de fichier NTFS :
  http://msdn.microsoft.com/en-us/library/windows/desktop/aa365230(v=vs.85).aspx
- Registre :
  http://msdn.microsoft.com/en-us/library/windows/desktop/ms724871(v=vs.85).aspx
- Que faire en cas d'intrusion ? :
  http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

2 - Risques liés au format Portable Executable (PE)

Le format PE est le format binaire des fichiers exécutables et des fichiers de code objet utilisés sur les systèmes d'exploitation Windows depuis Windows NT 3.1. Ce format a été introduit en 1993 dans le but de pouvoir supporter différentes architectures de processeurs et non pas uniquement l'architecture x86 comme cela était le cas avec le format précédent (« New Executable », ou NE). Son omniprésence dans une très large majorité des systèmes informatiques actuels, et ses caractéristiques techniques intéressantes, font de lui un format incontournable pour un attaquant. Il est observé dans quasiment tous les scénarios d'attaques, de la phase de primo infection (attaque initiale) jusqu'à l'objectif ultime de prendre la main à distance sur une ressource critique voire sur l'ensemble d'un parc informatique.

Le but de cet article est de sensibiliser le lecteur aux particularités du format PE, dont les risques sont souvent méconnus ou sous-estimés, et de l'amener à considérer ce format avec la plus grande attention dans une optique de sécurisation d'un poste ou d'un système d'information, au travers de quelques recommandations.

Un conteneur portable de code et de données

Le format PE contient tout ce qui est nécessaire à un programme pour être exécuté par le système d'exploitation, à savoir du code exécutable, et des données et ressources, auxquelles le code peut accéder facilement.

La nature du code contenu dans un fichier au format PE peut être variée. Il peut s'agir de :

- Fichiers exécutables (.EXE)
- Fichiers OLE ou activeX (.OCX)
- Bibliothèques dynamiques de code (.DLL)
- Éléments du panneau de configuration (.CPL)
- Économiseurs d'écran (.SCR)
- Modules noyau (.SYS)
- Fichiers « Extensible Firmware Interface » (.EFI)

Dans certains cas, un fichier PE peut contenir du code « interprétable », c'est-à-dire nécessitant une machine virtuelle pour être exécuté. Cela peut être par exemple du Visual Basic, du DotNet (.NET) ou de l'AutoIt (un langage de script de plus en plus populaire). En particulier, la technologie Silverlight, utilisée dans les modules de navigateurs Internet, s'appuie sur le format .NET, lui-même intégré au format PE. Les ressources peuvent quant à elles être par exemple des images, des polices, des informations de configuration, etc. Il est possible de trouver des fichiers PE qui ne contiennent pas de code (dits « code-less »), mais uniquement des ressources. C'est notamment le cas de certaines bibliothèques (.DLL) Windows.

Lorsqu'un fichier PE est chargé en mémoire depuis le disque par le « loader » Windows puis lancé, il est exécuté dans le contexte de l'utilisateur courant. Le code a donc les droits de cet utilisateur. Si l'utilisateur a des droits privilégiés (en particulier s'il est administrateur), le code les aura aussi. Ce format est donc très intéressant pour les attaquants, et une grande partie des compromissions de postes Windows implique un fichier PE malveillant, permettant le plus souvent d'en prendre le contrôle à distance.

La machine compromise peut alors être utilisée aux fins suivantes :

- Participation à des activités illégales au sein d'un réseau de machines zombies (« botnet ») ;
- Espionnage : récupération de données à caractère sensible et exfiltration à l'insu de son utilisateur ;
- Sabotage : dérèglement d'un programme informatique dans le but de nuire.

Un format difficile à analyser

Depuis ses débuts, le format PE a subi de nombreuses évolutions pour supporter les nouveaux systèmes d'exploitation (Windows XP / Vista / Seven / 8) et les nouvelles architectures matérielles (par exemple, l'évolution des processeurs de 32 à 64 bits, et plus récemment ARM) tout en restant rétro-compatible avec les systèmes les plus anciens. Par conséquent, de nombreuses fonctionnalités, qui ne sont plus utilisées aujourd'hui, sont toujours présentes. Ces fonctionnalités permettent une utilisation détournée du format PE, c'est-à-dire une utilisation qui n'est pas conforme aux spécifications officielles. De plus, certaines incohérences impliquent des comportements différents pour un même fichier PE selon le système d'exploitation Windows sur lequel il est exécuté. Deux principaux écueils rendent l'analyse de ce format difficile : d'une part, le concept d'image disque et d'image mémoire, avec la notion d'adresse mémoire virtuelle relative (« Relative Virtual Address », ou RVA), et d'autre part, la flexibilité du format et le manque de rigueur présent à la fois dans les spécifications et le « loader » Windows. En effet,

les spécifications officielles sont relativement récentes (2006) et le « loader » de Windows est très permissif, se révélant souvent non conforme aux spécifications officielles.

La RVA est une adresse mémoire relative à une adresse mémoire de base donnée, appelée base de l'image (« Image Base »). La plupart des adresses exprimées dans le format PE sont exprimées selon ce concept de RVA. Lorsque le fichier est analysé sur le disque, il est donc nécessaire d'effectuer des conversions pour obtenir les bonnes positions dans le fichier car l'image mémoire du fichier n'est pas la même que celle sur le disque à cause d'une granularité d'alignement différente des sections (typiquement 512 octets sur le disque contre 4096 octets en mémoire). De plus, le « loader » Windows des fichiers PE ne lit sur le disque que la moitié des en-têtes du format. L'autre moitié est lue en mémoire, après chargement. Cette singularité permet de forger des fichiers PE valides au sens de l'exécution, mais qui seront vus comme invalides par un outil d'analyse s'appuyant sur la représentation du fichier sur le disque.

Cette complexité du format et cette divergence entre les spécifications officielles et le « loader » de Windows rendent l'analyse statique (sans exécution) des fichiers PE difficile. Certains outils d'analyse comme les antivirus peuvent parfois être mis en défaut par des « malformations » de fichiers PE. Enfin, il existe des programmes, appelés « packers », capables de « protéger » et d'envelopper un PE (en utilisant notamment des fonctions de compression et de chiffrement), qui sont souvent utilisés de façon détournée par les attaquants pour donner une apparence légitime à un PE malveillant. Des programmes légitimes, souvent populaires et ayant la confiance des utilisateurs, peuvent également être détournés par adjonction de code

malveillant. En conséquence, bien que ce format soit incontournable pour le bon fonctionnement des systèmes, il est important de rester vigilant face à des fichiers PE d'origine inconnue ou non vérifiée.

Vecteurs de diffusion des PE malveillants

Les fichiers PE sont omniprésents aujourd'hui et peuvent être contenus dans des fichiers parents tels que des archives (.RAR, .ZIP), des installeurs (.MSI) ou tout autre type de conteneurs de données. Si cela peut sembler surprenant, rien n'empêche cependant d'embarquer des fichiers PE dans des documents qui ne sont pas a priori prévus à cet effet. Il est fréquent notamment d'observer des fichiers bureautiques (PDF, DOC, etc.) dont l'utilisation est détournée afin de piéger l'utilisateur, embarquant une charge utile malveillante au format PE.

Les vecteurs de diffusion de fichiers PE malveillants sont multiples, et bien les connaître aide à prendre les mesures de sécurité adéquates. On peut citer principalement l'envoi de courriels, la navigation sur Internet, et la diffusion par supports amovibles USB :

Les courriels

- Via une campagne de pourriels dont le but est d'inciter le destinataire à exécuter un fichier PE malveillant en le trompant sur la nature de la pièce jointe. On observe par exemple couramment des pièces jointes dont le nom se termine par « .pdf.exe » et dont l'icône correspond à un fichier PDF. Par défaut, les extensions de fichiers étant masquées sous Windows, l'utilisateur peu averti pense avoir affaire à un PDF. C'est par exemple le cas du maliciel « Upatre ».
- Via un courriel contenant un lien piégé. L'attaquant exploite alors des techniques d'ingénierie sociale (« phishing », « spear-phishing »), afin d'inciter le destinataire à cliquer sur ce lien qui le redirigera vers un site Web piégé.
- Via un courriel contenant un document en apparence légitime au format PDF ou DOC par exemple. L'attaquant incite son destinataire à ouvrir cette pièce jointe, spécialement formée afin d'exploiter une vulnérabilité des applications exploitant ce format, via des techniques d'ingénierie sociale. En cas d'exploitation réussie, un fichier au format PE est téléchargé et exécuté.

La navigation Internet

- Via un téléchargement délibéré par l'utilisateur d'un fichier PE (utilitaires et jeux par exemple, qui peuvent s'avérer piégés).
- Via la visite d'un site Internet légitime mais préalablement compromis et redirigeant la navigation vers un autre lien permettant l'exploitation d'une vulnérabilité du navigateur ou d'un de ses modules, et menant au téléchargement d'un PE malveillant (par exemple, grâce à l'utilisation de conteneur HTML de type « iFrame » de petite taille, afin qu'ils ne soient pas visibles pour l'utilisateur).
- Via un clic sur un lien piégé qui redirige l'internaute vers un site Web distribuant des fichiers PE malveillants. Les réseaux sociaux sont notamment de plus en plus exploités par les attaquants à cette fin, d'une part car ils sont aujourd'hui massivement utilisés, et d'autre part car les utilisateurs sont moins méfiants. L'utilisation

grandissante de réducteurs d'URL, rendant celles-ci inintelligibles à leur simple lecture accroît un peu plus encore le risque de se faire piéger.

– Via des fenêtres surgissantes (« popups ») dans le navigateur. La stratégie consiste généralement à faire croire à la nécessité d'un téléchargement (module requis pour l'affichage correct de la page ou le visionnage d'une vidéo par exemple), ou repose sur la peur en prétendant qu'un virus a été détecté sur le poste et en proposant le téléchargement d'un antivirus, qui se révèle en fait être un maliciel au format PE (généralement appelé « rogue »).

Les supports amovibles USB

– Les supports amovibles USB tels que les clés de stockage, les disques durs externes ou les chargeurs de téléphone constituent un autre vecteur d'infection, notamment par le biais de l'exécution automatique (« autorun ») qui permet de lancer directement un fichier PE contenu sur le support.

Comment se protéger ?

En théorie, il ne faudrait jamais exécuter un fichier PE dont la provenance n'a pas pu être vérifiée. Cependant, cela n'est pas toujours simple dans la pratique. Néanmoins, il est possible de réduire significativement les risques en suivant les recommandations ci-dessous :

– Filtrer les fichiers PE dans les mails ;
– maintenir les systèmes d'exploitation et les logiciels à jour (à commencer par les plus courants, comme Adobe Reader et Flash, Java, Internet Explorer, etc.) ;
– avoir un antivirus sur les postes de travail à jour avec une protection résidente active, et de préférence intégrant des technologies avancées, comme l'émulation, permettant de détecter de façon générique des comportements suspects ou malveillants, et non seulement certaines signatures déjà connues ;
– ne pas accéder à l'Internet depuis un compte privilégié, et utiliser de préférence un environnement séparé pour la navigation Internet, spécifié selon le risque identifié (poste dédié, utilisation d'environnements virtuels, etc.) ;
– éviter dans la mesure du possible de se connecter aux réseaux sociaux depuis un poste professionnel ;
– désactiver l'exécution automatique (« autorun ») des supports amovibles ;
– utiliser des modules complémentaires renforçant la sécurité du navigateur Internet, en bloquant par exemple les fenêtres surgissantes ou en limitant l'exécution du code Javascript (ex : NoScript) ;
– télécharger les fichiers PE nécessaires depuis le site de l'éditeur afin d'éviter de récupérer une version modifiée par un tiers potentiellement malveillant. La signature digitale, quand elle est présente, doit être vérifiée pour augmenter la confiance (de même que la conformité du condensat du fichier avec celui annoncé par l'éditeur). Une absence de signature digitale devrait aujourd'hui attirer l'attention de l'utilisateur : tous les logiciels des éditeurs importants du marché sont signés.
– Rendre l'exploitation de vulnérabilités plus difficile en configurant les logiciels avec des paramètres de sécurité renforcés (activation des fonctionnalités bacs à sable ou « sandbox » pour les programmes qui en sont pourvus, utilisation du logiciel EMET de Microsoft, etc.).
– Mettre en place des restrictions logicielles (en utilisant les SRP ou AppLocker sous Windows, pour par exemple empêcher l'exécution de programmes depuis des clés USB) ;
– Sauvegarder les données régulièrement afin de disposer à tout moment d'un duplicat. En effet, certains maliciels appelés rançongiciels (« ransomwares ») peuvent chiffrer des données personnelles présentes sur la machine de la victime afin de lui demander une somme d'argent en échange d'une clé de déchiffrement.
– Sensibiliser et éduquer les utilisateurs à ces menaces pour éviter la compromission mais également être capable de repérer un poste compromis et de prendre les dispositions nécessaires rapidement.

Documentation

– MSDN Microsoft PE and COFF Specification :
http://msdn.microsoft.com/en-us/windows/hardware/gg463119.aspx
– Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows :
http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf

3 - Mises à jour non officielles de Windows XP

Depuis le 8 avril 2014, Microsoft ne publie plus de mises à jour de sécurité pour son système d'exploitation Windows XP et la suite bureautique Office 2003. Récemment, une méthode a été diffusée sur Internet permettant de recevoir des mises à jour via Windows Update jusqu'en 2019.

Risques liés aux correctifs non officiels

La méthode précédemment citée consiste à modifier la configuration de Windows XP afin d'utiliser le service de mise à jour de la version dédiée aux systèmes embarqués. Ainsi, le système recevra et appliquera les mises à jour publiées pour ce système dont l'arrêt du support est prévu pour 2019.

Les futures mises à jour publiées pour ce système ne seront pas adaptées aux versions de Windows XP installées sur les postes de travail. L'application de ces correctifs sur de telles installations comporte de nombreux risques tels que :

- l'instabilité du système : ces mises à jour ne sont pas testées quant à la présence d'effets de bord sur les versions pour poste de travail ;
- la non-correction des failles : ces mises à jour ont pour but de corriger des failles de sécurité spécifiques aux systèmes embarqués et non à la version pour postes de travail. Les postes de travail ainsi modifiés ne seront donc pas forcément protégés contre les futures vulnérabilités identifiées impactant Windows XP.

Recommandations

Le CERT-FR recommande de ne pas utiliser de méthode permettant de contourner les restrictions mises en place au niveau du service de mise à jour et de ne pas chercher à recevoir des correctifs dédiés à une autre version du système d'exploitation.

De plus, le CERT-FR alerte les utilisateurs sur le potentiel danger lié à la publication de faux correctifs pour des logiciels qui ne sont plus supportés par leur éditeur. En effet, des personnes malintentionnées peuvent être tentées de diffuser des codes malveillants en les faisant passer pour des correctifs. Dans ce cadre, le CERT-FR attire l'attention sur le fait qu'il est important de n'appliquer que des correctifs officiels publiés par l'éditeur.

Plus généralement, le CERT-FR recommande de migrer les équipements encore sous Windows XP vers des systèmes d'exploitation supportés par leurs éditeurs afin de pouvoir bénéficier des derniers correctifs de sécurité.

Documentation

- Recommandations de l'ANSSI sur l'arrêt du support de Windows XP :
  http://www.ssi.gouv.fr/fr/menu/actualites/arret-du-support-de-windows-xp-recommandations.html
- Bulletin d'actualité du CERTA sur les nouvelles fonctionnalités de sécurité dans Windows 8.1 :
  http://www.cert.ssi.gouv.fr/site/CERTA-2013-ACT-042/
- Annonce de la fin du support de Windows XP :
  http://windows.microsoft.com/fr-fr/windows/end-support-help

4 - Rappel des avis émis

Dans la période du 23 au 29 mai 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-240 : Multiples vulnérabilités dans TYPO3 CMS
- CERTFR-2014-AVI-241 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-242 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2014-AVI-243 : Vulnérabilité dans Apache Tomcat
- CERTFR-2014-AVI-244 : Multiples vulnérabilités dans Oracle Solaris
- CERTFR-2014-AVI-245 : Multiples vulnérabilités dans Samba
- CERTFR-2014-AVI-246 : Multiples vulnérabilités dans les produits Citrix

Gestion détaillée du document

30 mai 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-022`