

Cours sur Random System Information Tool

Par Sayce,

!! Certaines choses, notamment sur la partie registre ne sont pas détaillées/expliquées, il faut donc un minimum de connaissances sur le fonctionnement du registre, et sur le fonctionnement d'un système d'exploitation pour pouvoir comprendre ce cours!!

Random System Information Tool, a été créé après HijackThis par Random/Random , justement parce que ce dernier n'évoluait plus, et que certaines zones non scannées par HijackThis étaient nécessaires pour une bonne désinfection de certains malwares.

Ce logiciel est vraiment un bon logiciel, car il donne de nombreux renseignements, il ne crée pas de clé dans le registre, seulement un dossier nommé «rsit» à la racine du disque dur pour y stocker les deux rapports qu'il génère, il est très simple d'utilisation, et ne propose pas de fonction de suppression, donc aucun risque pour l'utilisateur.

Le logiciel Random System Information Tool après son scan génère deux rapports, le rapport info.txt, et le rapport log.txt. Nous allons analyser en détail ces deux rapports. A noter, que si on le lance plusieurs fois, il ne génère plus que le rapport log.txt.

log.txt :

Ce rapport se découpe en plusieurs parties :

#

Il débute par un en-tête proposé par Random System Information Tool .

Exemple :

*Logfile of random's system information tool 1.08 (written by random/random) **Version de***

Random System Information Tool

*Run by Sayce at 2010-07-24 18:26:54 **Nom de l'utilisateur/date/heure***

*Microsoft Windows XP Édition familiale Service Pack 3 **Version du système d'exploitation***

*System drive C: has 31 GB (84%) free of 37 GB **Taille du disque dur principal/Pourcentage de libre***

*Total RAM: 495 MB (50% free) **Taille de la mémoire vive/Pourcentage de libre***

Explications :

Présentes en gras à la fin de chaque ligne.

Regardez bien les deux dernières lignes, elles peuvent expliquer un ralentissement du PC. En effet sur les forums on est souvent confrontés à des utilisateurs ayant un PC ralenti, et on se lance alors dans une désinfection. Mais les ralentissements ne sont pas toujours dû à une infection, ils peuvent être dû au fait que le PC est trop plein, trop de logiciels lancés en même temps pour peu de mémoire vive ..

##

Il s'ensuit un rapport HijackThis entier, et normal, car Random System Information Tool télécharge

HijackThis sur le PC pour qu'il génère un rapport.
Je ne vais pas vous détailler les lignes du rapport HJT, il y a un excellent cours sur BleepingComputer <http://www.bleepingcomputer.com/tutorials/tutorial123.html>

###

Puis viens une listes des «*Scheduled tasks folder*», c'est-à-dire des tâches planifiées. Les tâches planifiées permettent d'exécuter automatiquement des tâches à un moment précis. Il faut bien les vérifier, car bien souvent les infections créer des tâches planifiées pour par exemple se lancer à certains moments précis. Les tâches planifiées sont des fichiers portant l'extension .job.

Exemple :

C:\WINDOWS\tasks\AppleSoftwareUpdate.job

Explications :

Bon, et bien ce n'est pas très dur, il y a donc une tâche planifiée présente au chemin indiqué, apparemment créée par le logiciel de mise à jour de Apple. Elle finie, comme souligné précédemment, par .job.

####

Ensuite, la partie «*Registry dump*», qui contient une liste de nombreuses clés registre étant souvent utilisées par les infections.

Je vous conseille de faire très attention à cette partie, car elle permet de repérer les fichiers/clés/dossiers .. créés/modifiés par l'infection, et donc de l'éradiquer complètement.

>< [*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects*

Cette clé contient la liste de toutes les BHO. Une BHO «*Browser Helper Object*» est une petite application tierce (de type "plug-in") qui, une fois installée, ajoute des fonctionnalités (désirées ou non) à Internet Explorer. Certaines BHO sont nuisibles, il faut donc bien regarder cette clé. Le navigateur, que ce soit Internet Explorer, Firefox ou un autre, et un élément important pour la sécurité du PC. En effet c'est lui qui fait le lien PC/Internet, sachant que l'internet apporte la grande majorité des infections, il est essentiel de surveiller ce qui s'installe sur la navigateur. Les Browser Helper Object par conséquent s'installent sur la navigateur, et modifient son apparence, mais peuvent aussi le manipuler à leur guise par exemple, elles peuvent enregistrer les sites sur lesquels vous allez, ou encore modifier votre page d'accueil et afficher des pop-ups ...

Je vous conseille de lire ceci : <http://forum.malekal.com/bho-plugins-add-ons-sur-internet-explorer-t7959.html>

Exemple :

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{25147105-f2aa-4be2-8a71-ac68a4bfa05c}

C:\WINDOWS\system32\wpyugv.dll [2008-11-12 113664]

Explications :

La clé habituelle, à laquelle un CLSID (http://fr.wikipedia.org/wiki/Globally_Unique_Identifier) permettant de reconnaître la Browser Helper Object est ajouté en sous-clé. Puis, en donné, le fichier .dll de la Browser Helper Object est indiqué suivi de la date de sa création et de sa taille. Vu le nom aléatoire de la .dll, la Browser Helper Object est infectieuse.

>> [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar]

Cette clé contient la liste de toutes les barre d'outils. Les toolbars, «barre d'outils», sont des barres qui s'ajoutent sur les navigateurs, et qui permettent des fonctionnalités en plus. La majorité du temps ces barres d'outils ne portent que peu d'intérêts, et alourdit le PC, et la navigation. Néanmoins de très nombreux internautes ont de très nombreuses barres d'outils sur leurs PC, les installant avec des logiciels qui les proposent lors de leur propre installation.

Exemple :

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Toolbar\{EE5D279F-081B-4404-994D-C6B60AAEBA6D}]
- EPSON Web-To-Page - C:\Program Files\EPSON\EPSON Web-To-Page\EPSON Web-To-Page.dll [2005-02-21 368640]

Explications :

La clé habituelle, à laquelle un CLSID (http://fr.wikipedia.org/wiki/Globally_Unique_Identifier) permettant de reconnaître la barre d'outil est ajouté en sous-clé. Ensuite vient le nom de la barre d'outil . Puis en donné, le fichier .dll de la barre d'outil ici la barre d'outil appartient à Epson, elle est donc légitime.

>> [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]

Cette clé liste les logiciels ce lançant via la clé «Run». Cette clé permet de lancer les logiciels au démarrage. Clé très importante, quand on sait que la majorité des infections ce lance dès le démarrage du PC.

Exemple :

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"QuickTime Task"=C:\Program Files\QuickTime\qttask.exe [2008-03-28 413696]

Explications :

En 1er ligne on voit la clé Run, puis entre «», la valeur mise sous l'effigie de la clé, puis à droite du «=» ce trouve la donnée assignée à la valeur, suivit de la date de sa création, puis de sa taille. Pour vérifier la légitimité, on utilise le fichier, ici «*qttask.exe*», ou le nom de la valeur «*QuickTime Task*». N'oubliez pas de regarder la date de création, lors d'une infection les fichiers infectieux sont tous créer dans la même période.

>> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]

Pareil que la précédente, sauf que la ruche change, ici c'est «HKCU»

Pas d'exemple ici , c'est la même chose que la précédente, seul la ruche change.

>> [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\]

Liste les services qui ce lancent lors du démarrage sans échec.

>>[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\network\]

Liste des services qui ce lancent lors du démarrage en mode sans échec prise ne charge du réseau

>> [HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\]

Liste tous les logiciels autorisés par msconfig au démarrage, (Visible aussi via msconfig dans la ligne de commande Exécuter).

>> [HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupfolder\]

Liste des programmes du dossier démarrage «C:\Documents and Settings\NOMDESESSION\Menu Démarrer\Programmes\Démarrage» sous XP, et sous Vista., «C:\User\NOMDESESSION». Ce

dossier de démarrage permet de lancer un fichier .ink (raccourcis), qui a son tour lance le .exe dont il est le raccourcis.

><

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\]
```

Liste des fichiers ce lançant dès l'ouverture de session.

Exemple :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\vtUkljg]  
vtUkljg.dll []
```

Explications :

La 1er ligne est la clé listé, c'est à dire HKLM/..../Notify suivit de «vtUkljg» en sous-clé, puis en 2ém ligne, la donné assigné à la clé. Ici la clé/donné sont infectieuses. Vous remarquerez qu'il n'y a pas date entre les crochets, ceci signifie souvent, mais pas tout le temps que la clé est orpheline, c'est à dire que la donné n'existe pas et donc la clé ne renvoie vers rien. Mais le fait que les crochets soit vides, peut être dut à un mauvaise accès au fichier ou autre.

><

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad]
```

Liste des fichiers lancés par Explorer.exe

><

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
```

Liste des restrictions/stratégies de sécurité. Ces restrictions peuvent être utilisées par les administrateurs dans certains lieu de travail pour empêcher l'accès à certaines options sur le PC, mais elles sont aussi souvent utilisées par les malwares pour empêcher l'accès à la BDR par exemple, ou au gestionnaire des taches.

Exemple :

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]  
"dontdisplaylastusername"=1  
"legalnoticecaption"=
```

Explications :

La première ligne correspond à la clé. La deuxième ligne correspond à une restriction nommé « dontdisplaylastusername » qui a pour but de déterminer si le nom du dernier utilisateur doit être conservé pour la prochaine ouverture de la session. Comme vous le voyez elle a pour donné «1», le plus souvent (Pas tous le temps.) lorsque les restrictions on pour donné 1, elles sont active, et quand elles ont pour donné «0» elles sont inactives.

Et la troisième ligne correspond à une restriction nommé «legalnoticecaption». Cette fois la restriction na pas de donné c'est parce que souvent les données vide sont les données par défaut. Alors ces deux restrictions ne sont pas dangereuses, mais celle-ci «DisableTaskMgr» permet de désactiver le gestionnaire des taches, et empêche à l'utilisateur d'y accéder. Ceci permet à l'infection d'empêcher l'utilisateur de regarder les processus lancés, et donc de vérifier si le PC est infecté. Donc, comme vous le voyez les restrictions peuvent être intéressantes à utiliser pour les malwares. L'infection Smitfraud/Zlob utilise beaucoup les restrictions.

><

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\explorer]
```

Comme la précédente, seule la dernière sous clé change, ici c'est «explorer» au lieu de «system»

><

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\explorer]
```

Comme la précédente, seule la ruche change, ici c'est «HKCU».

><

```
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\standardprofile\authorizedapplications\list]
```

Liste les applications autorisées par le firewall de Microsoft. En effet, les applications doivent demander l'accès au net au firewall de Microsoft (Si il est le Firewall du PC), et donc les malwares sont souvent présent dans cette clé du fait qu'ils ont souvent besoin d'avoir un accès au net.

Exemple :

```
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy\domainprofile\authorizedapplications\list]
```

```
"C:\Program Files\Windows Live\Messenger\msnmsgr.exe"="C:\Program Files\Windows Live\Messenger\msnmsgr.exe:*:Enabled:Windows Live Messenger"
```

Explications :

Cette ligne signifie donc que le logiciel MSN a le droit d'accéder à internet.

En effet la première ligne correspond à la clé d'autorisation à l'accès au net, les autres montrent quels fichiers aura accès au net. **[VERIFIER]**

><

```
[HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\mountpoints2\]
```

Cette clé permet de voir quel périphérique a été connecté au PC, et donc de déceler une infection par support amovible. Clé très importante.

Exemple :

```
[HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\mountpoints2\{410476de-2cf3-11dd-9a4d-001d926d047f}]
```

```
shell\AutoRun\command - E:\RavMon.exe
```

```
shell\explore\command - E:\RavMon.exe -e
```

```
shell\open\command - E:\RavMon.exe
```

Explications :

Le CLSID attaché à notre clé de départ est un identifiant propre à chaque support amovible.

La deuxième ligne correspond au fichier Autorun du support amovible. Le fichier Autorun permet de lancer automatiquement la clé lorsqu'on la branche au PC, c'est via ce fichier que les infections par supports amovibles se propagent. Ici le fichier s'appelle «RavMon.exe», une simple recherche sur le net permettra de déterminer que c'est infectieux.

La troisième ligne correspond à l'ouverture du support amovible par clique droit // Explorer

La quatrième ligne correspond à l'ouverture de support amovible par double clique gauche.

On en déduit donc que ces supports amovibles sont infectés, il faudra donc lors de la désinfection les brancher au PC, pour pouvoir les nettoyer.

#####

Viens ensuite la liste des fichiers/dossiers créer «*List of files/folders created in the last 1 months*», et modifiés «*List of files/folders modified in the last 1 months*» le dernier moi (réglage par défaut) ou les 2 ou 3 derniers mois. Cette listes permet de repérer les fichiers crée par l'infection depuis sont installation.

Lors de la liste des fichiers/dossiers créaient/modifiaient, apparaît en début de ligne la date/l'heure de création du fichier dossier.

Suivit de une ou plusieurs lettres, qui indique si c'est un fichier/dossiers, et les attributs de ce fichier/dossier; voici les lettres possiblement affichées :

La lettre «D» pour Directory (Dossier) ce qui signifie que l'objet en fin de chemin est un dossier.

La lettre «S» pour System (Système) signifie que le fichier/dossier est un fichier/dossier système.

La lettre «H» pour Hidden (Caché), qui signifie que le fichier/dossier est un fichier/dossier caché.

La lettre «R» pour Read only (Lecture seule), qui signifie que le fichier/dossier est un fichier/dossier en lecture seul.

La lettre «A» pour Archive (Archive), qui signifie que le fichier/dossier est une archive.

La lettre «N» pour Normal (Normal), qui signifie que le fichier ne comporte pas d'attribut.

Exemple :

2008-11-12 20:38:26 ----RSH---- C:\WINDOWS\SVCHOST.EXE

Explications :

«*2008-11-12 20:38:26*» Date et heure de la création du fichier

«*RSH*» Indique que, c'est un fichier en système, en lecture seul et caché.

«*C:\WINDOWS\SVCHOST.EXE*» Indique le chemin du fichier crée, c'est à dire svchost.exe

#####

Et enfin, pour finir, RSIT nous expose une liste des pilotes «*List of drivers*» et des services «*List of services*».

L'état du service/pilote :

La lettre «R» signifie que le service/pilote est démarré (Running)

La lettre «S» signifie que le service/pilote est stoppé (Stopped)

Le type de démarrage du service/pilote

Le nombre «0» signifie qu'il est lancé au démarrage du PC

Le nombre «1» signifie qu'il est lancé au démarrage du système

Le nombre «2» signifie qu'il est lancé automatiquement

Le nombre «3» signifie qu'il n'est lancé que manuellement.

Le nombre «4» signifie qu'il est désactivé.

Type de ligne

Lettre/Chiffre NomRéalDuService(Nom

d'usage)/pilote;NomDuService(ServiceName)/piloteAffiché;CheminDuFichier [DateDeCréation

TailleDuFichier]

Exemple de service :

R2 AntiVirSchedulerService;Avira AntiVir Planificateur; C:\Program Files\Avira\AntiVir Desktop\sched.exe [2009-05-13 108289]

Explication :

«R2» : Le service est démarré, et ce lance avec le système.

«AntiVirSchedulerService» : Nom réel du service.

«Avira AntiVir Planificateur» : Nom du service affiché (nom souvent plus simple que le réel)

«C:\Program Files\Avira\AntiVir Desktop\sched.exe» : Fichier exécutable associé au service.

«[2009-05-13 108289]» : Date de création du service (Quand il n'y a pas de date, il y a des chances que le fichier n'existe plus.) Le chiffre qui suit correspond à la taille du fichier en octets.

Passons au deuxième rapport, beaucoup plus simple :

info.txt :

Celui-ci aussi, ce scinde en plusieurs parties, et nous allons aussi les détailler :

#

La première partie du rapport ce nomme «Uninstall list», et contient la liste des logiciels présents dans Ajouts/Suppression de programmes (Sous XP), Programmes (Sous Vista/Seven).

Cette liste permet de voir si il y a des logiciels de P2P, de cracks, ou encore plusieurs antivirus, même si l'on aperçoit souvent ces logiciels dans le rapport log.txt, cela permet d'être sûr de tout voir.

Exemple :

```
Apple Software Update-->MsiExec.exe /I{B74F042E-E1B9-4A5B-8D46-387BB172F0A4}
avast! Antivirus-->C:\Program Files\Alwil Software\Avast4\aswRunDll.exe "C:\Program
Files\Alwil Software\Avast4\Setup\setiface.dll",RunSetup
```

Explications :

La première ligne correspond au logiciel de mise à jour de Apple, et indique le fichier exécutable utilisé pour mettre à jour Apple. Ce fichier, est un fichier appartenant à Windows permettant de mettre à jour les logiciels fournis avec Windows.

La deuxième ligne nous montre que le logiciel Avast est installé sur le PC, elle nous montre aussi que le fichier «aswRunDll.exe» lance le fichier «aswRunDll.exe». Il arrive souvent que vous ayez ce genre de ligne dans les rapports HijackThis, un premier fichier légitime, qui en lance un second entre «» qui lui est parfois illégitime, donc lors de la désinfection si elle est manuelle, ne supprimer que le 2ème fichier.

##

La deuxième partie nous donne un aperçu du fichier host, nommé «Hosts File». Le fichier Host, est un fichier texte qui se trouve ici «C:\Windows\System32\drivers\etc\host». Ce fichier texte permet à votre ordinateur de faire la correspondance entre un nom de domaine (google.com) et une adresse IP (216.109.118.69). En effet, lorsque vous vous connectez à une site web, l'ordinateur utilise non pas au site grâce à l'adresse littérales, mais grâce à l'adresse ip.

Les fichiers host sont aussi utilisés par les infections, car ils peuvent permettre de rediriger les recherches. Mettons que vous souhaitiez vous connecter sur le site d'Avira AntiVir, pour le télécharger, et bien, le malware aura pu modifier le fichier host de tel sorte à vous empêcher l'accès au site web de Avira AntiVir. Il est donc important de scanner le fichier host, pour déceler tel ou tel détournement de surf.

Exemple :

127.0.0.1 localhost

127.0.0.1 mpa.one.microsoft.com

127.0.0.1 rad.msn.com

Explications :

La première ligne indique que l'adresse du pc est «127.0.0.1», c'est toujours la même, pour tout les PC, cette adresse est, comme indiqué à coté, l'adresse locale.

La deuxième ligne indique que **[VOIR]**

La troisième ligne indique que **[VOIR]**

###

La troisième partie «Security center information», centre de sécurité d'information. Cette partie liste les dernières alertes émisent par le centre de sécurité de Windows.

Exemple :

AV: AntiVir Desktop (outdated)

Explications :

Cette ligne nous montre que l'AV du PC, ici Avira AntiVir, n'est pas à jour, et que donc le PC cour un risque.

####

Cette troisième partie correspond «System event log», c'est à dire au journal des événements de Windows.

Le journal d'événement de Windows permet de lister les événements réalisé par Windows (comme une MAJ de Windows par exemple). Ce journal permet de visualiser les plantages d'applications, les problèmes de périphériques ...

Le journal d'événement est composé de trois parties, Application (événements enregistrés par les application), Sécurité (événements liés aux ouvertures de sessions et à l'utilisation des fichiers) et Système (événements lies aux composants de Windows) .

Il existe aussi trois types d'événements, Informations (descriptions du fonctionnement normale d'une application ..) Avertissement (descriptions d'un événement pouvant entraîner à une erreur) , et Erreur (description d'une erreur grave).

Les fichiers journaux ce trouvent ici : «%SystemRoot%\System32\Config» (.evt)

On peut accéder à l'observateur comme ceci :

Cliquer sur démarrer // Exécuter // inscrivez ceci 'eventvwr.msc' (Sans les ").

Je vous laisse consulter ceci : <http://forum.malekal.com/observateur-evenements-t12376.html>

Exemple :

Type de l'événement : Erreur <Type d'événement survenue, ici Erreur, niveau maximum de gravité.

Source de l'événement : Windows Update Agent <Application à l'origine de l'erreur

Catégorie de l'événement : Synchronisation logicielle <Niveau de gravité définie par la source de l'erreur.

ID de l'événement : 16 <Numéro permettant d'identifier le type de l'événement.

Date : 26/07/2010 <Date ou c'est produit l'ereur

Heure : 18:07:42 <Heure ou c'est produit l'erreur

Utilisateur : N/A <Utilisateur qui est à l'origine de l'événement.

Ordinateur : SAYCE-PC <Nom du PC ou c'est déroulé le problème.

Description : Connexion impossible, Windows ne parvient pas à se connecter au service Mises à

jour automatiques et ne peut donc pas procéder au téléchargement et à l'installation des mises à jour définies par la planification. Windows continuera d'essayer d'établir la connexion. <

Description de l'événement.

Explications :

Ceci, est une alerte présente dans le journal des événements. J'y ai inscrit ce que fait chaque lignes.

#####

La cinquième partie nommée «*Environment variables*», variables d'environnement, fait une liste des variables d'environnement présentes sur le PC. Les variables d'environnements sont des variables utilisées par le système d'exploitation pour pointer vers certains chemins.

En effet, prenons la variable «%temp%», cette variable pointe vers les dossiers des fichiers temporaires. Les dossiers ne se trouvant pas toujours au même endroit sur les ordinateurs, on utilise cette variable pour être sûr de bien supprimer les fichiers temporaires. Si elles n'existaient pas, il faudrait trouver les dossiers temporaires du PC, pour pouvoir ensuite supprimer les fichiers temp.

La variable «%allusersprofile%» indique le dossier du profil de tous les utilisateurs.

La variable «%ProgramFiles%» indique le dossier des logiciels installés.

La variable «%SystemRoot%» indique l'emplacement des fichiers systèmes ... Il en existe bien d'autres, celle-ci ne sont que des exemples. Retenez donc bien, que ces variables permettent de pointer vers un endroit précis du disque dur, et sont universelles sur les systèmes Windows.

Il est possible de créer des variables d'environnement, il est donc aussi possible aux malwares de créer leurs propres variables d'environnement, voilà pourquoi Random System Information Too nous liste les variables, pour nous permettre de voir si des variables infectieuses ont été créées.

Exemple :

```
"ComSpec"=%SystemRoot%\system32\cmd.exe
```

```
"TEMP"=%SystemRoot%\TEMP
```

Explications :

La première ligne signifie que «% ComSpec%» remplace le chemin

«C:\WINDOWS\system32\cmd.exe» (En effet, «%SystemRoot%» pointe vers «C:\WINDOWS».)

La deuxième ligne montre que la variable «%TEMP%» pointe vers «C:\WINDOWS\TEMP», cette variable est très utile. En effet, lors d'une désinfection si l'on a besoin de vider les dossiers temporaires, on utilise cette variable.

Voilà, c'est la fin de ce cours sur la lecture des rapports de Random System Information Too. Je n'ai pas intégré de contenu sur l'utilisation de RIST, le net en regorge, a vous de les chercher sur net, ou de vous faire vos propres cannes.

J'espère que ce cours vous aura plus, et vous aura aidé. Si vous avez des questions n'hésitez pas à me contacter par e-mail : sayce_simon[AROBASE]hotmail.fr