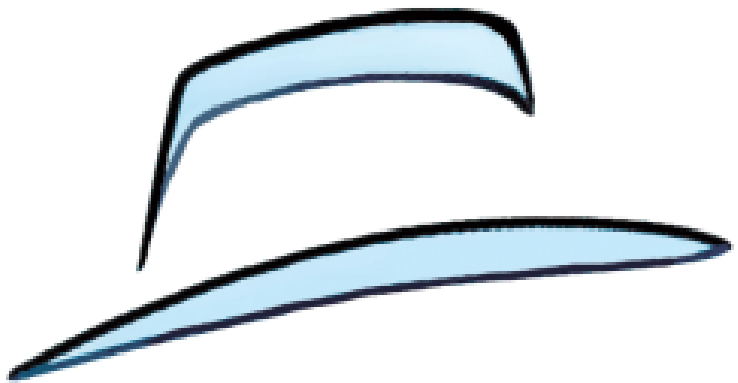
SysInternals

Éric BERTHOMIER
eric.berthomier@free.fr

March 16, 2022



Version 1.1 - Version Stagiaire

Présentation de la suite SysInternals

SysInternals est

- Une suite d'outils système et réseau

Présentation de la suite SysInternals

SysInternals est

- Une suite d'outils système et réseau
- Une suite d'outils Microsoft

Présentation de la suite SysInternals

SysInternals est

- Une suite d'outils système et réseau
- Une suite d'outils Microsoft

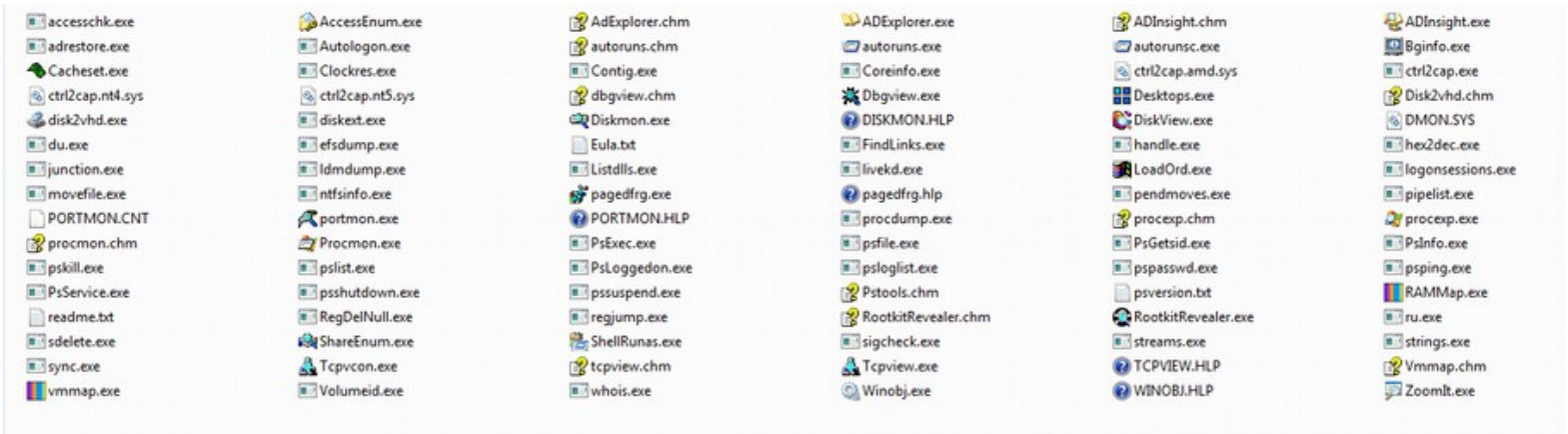
Présentation de la suite SysInternals

SysInternals est

- Une suite d'outils système et réseau
- Une suite d'outils Microsoft

SysInternals n'est pas

- Un outil de sécurité en tant que tel (bien que certains éléments le sont)



3 Outils parmi tant d'autres

- Autoruns

3 Outils parmi tant d'autres

- Autoruns
- ProcessExplorer

3 Outils parmi tant d'autres

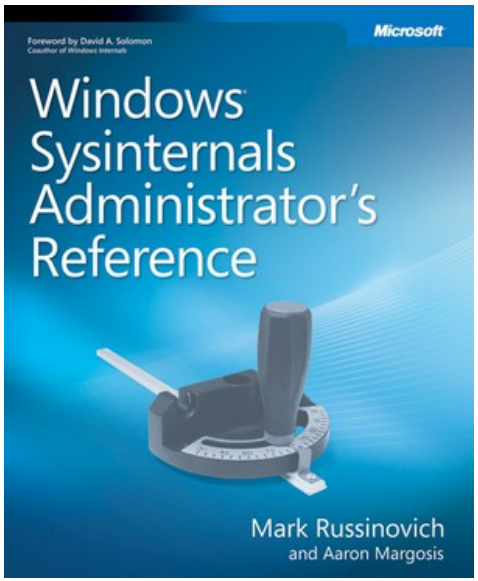
- Autoruns
- ProcessExplorer
- TcpView

3 Outils parmi tant d'autres

- Autoruns
- ProcessExplorer
- TcpView

3 Outils parmi tant d'autres

- Autoruns
- ProcessExplorer
- TcpView



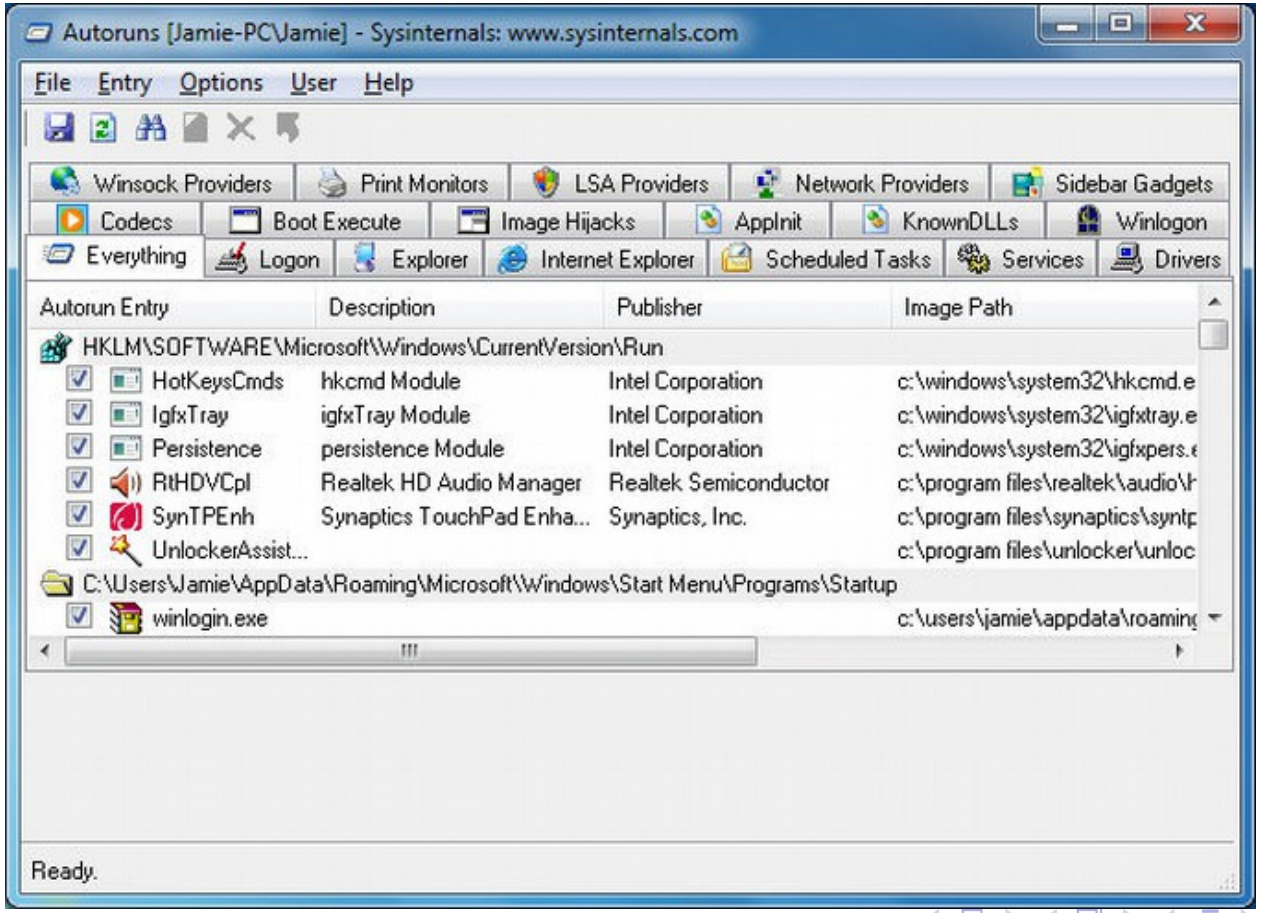
494 pages
Formation de 5 jours . . .

Autoruns

Autoruns est l'équivalent de `msconfig.exe` en amélioré. [1]

Autoruns

Autoruns est l'équivalent de `msconfig.exe` en amélioré. [1]



Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Autoruns permet de :

- Pour chaque élément, le

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Autoruns permet de :

- Pour chaque élément, le
  - Désactiver

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Autoruns permet de :

- Pour chaque élément, le
  - Désactiver
  - Supprimer

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Autoruns permet de :

- Pour chaque élément, le
  - Désactiver
  - Supprimer
  - Analyser

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Autoruns permet de :

- Pour chaque élément, le
  - Désactiver
  - Supprimer
  - Analyser
- D'enregistrer ń l'état de démarrage ż à un instant t pour le comparer par la suite

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.

Autoruns permet de :

- Pour chaque élément, le
  - Désactiver
  - Supprimer
  - Analyser
- D'enregistrer ń l'état de démarrage ż à un instant t pour le comparer par la suite

Ce que permet Autoruns

Autoruns peut nécessiter des droits d'Administration pour effectuer certaines modifications.
Autoruns permet de :

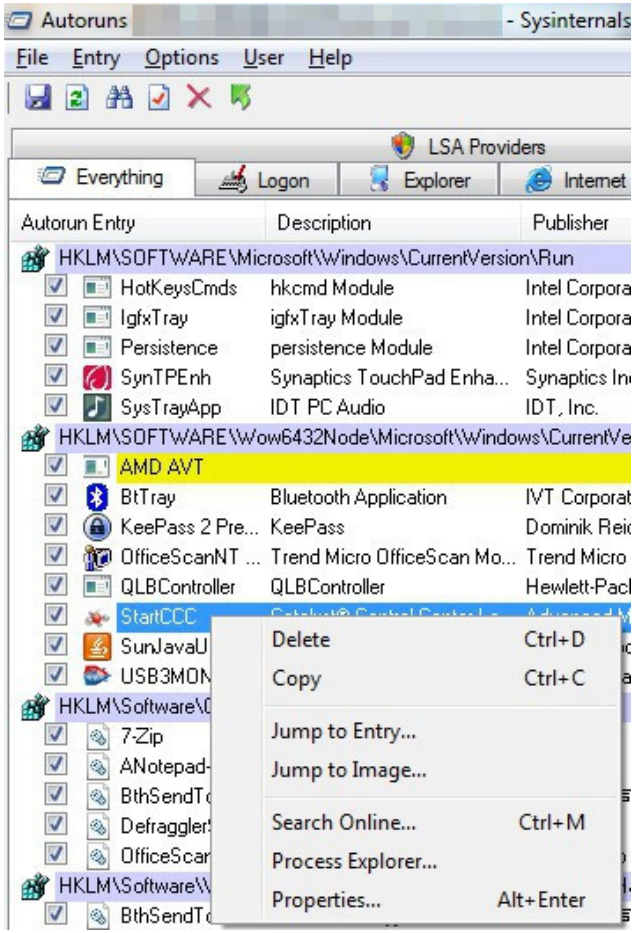
- Pour chaque élément, le
  - Désactiver
  - Supprimer
  - Analyser
- D'enregistrer ń l'état de démarrage ż à un instant t pour le comparer par la suite

D'où provient l'information ?

La vérité est qu'il existe de nombreuses localisations dans la base de registres et dans le système de fichiers qui peuvent être utilisées pour exécuter un programme au démarrage.

Actions sur une entrée

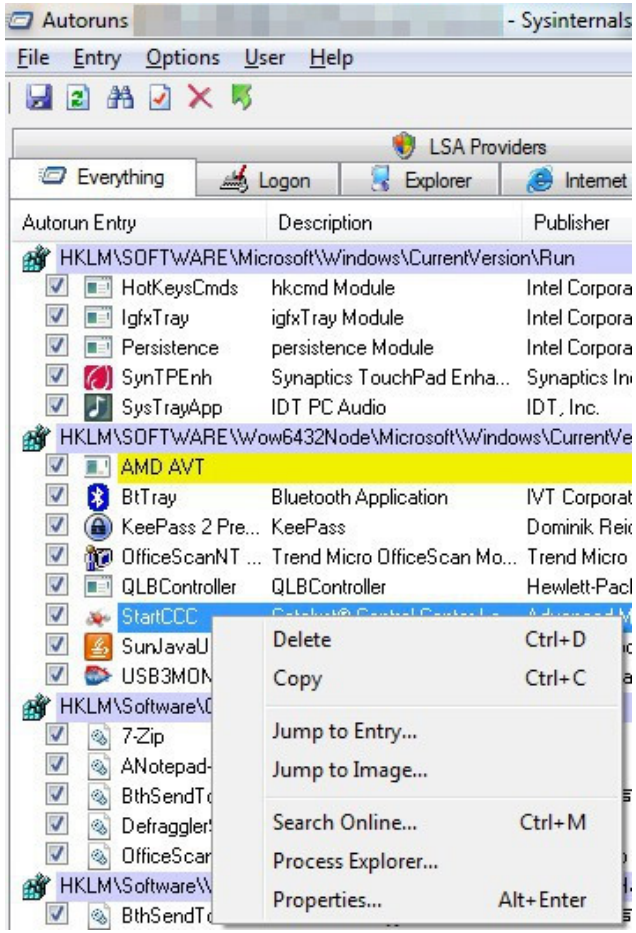
Delete Suppression de l'entrée



Actions sur une entrée

Delete Suppression de l'entrée

Copy Copie l'ensemble des informations lié à l'Entrée

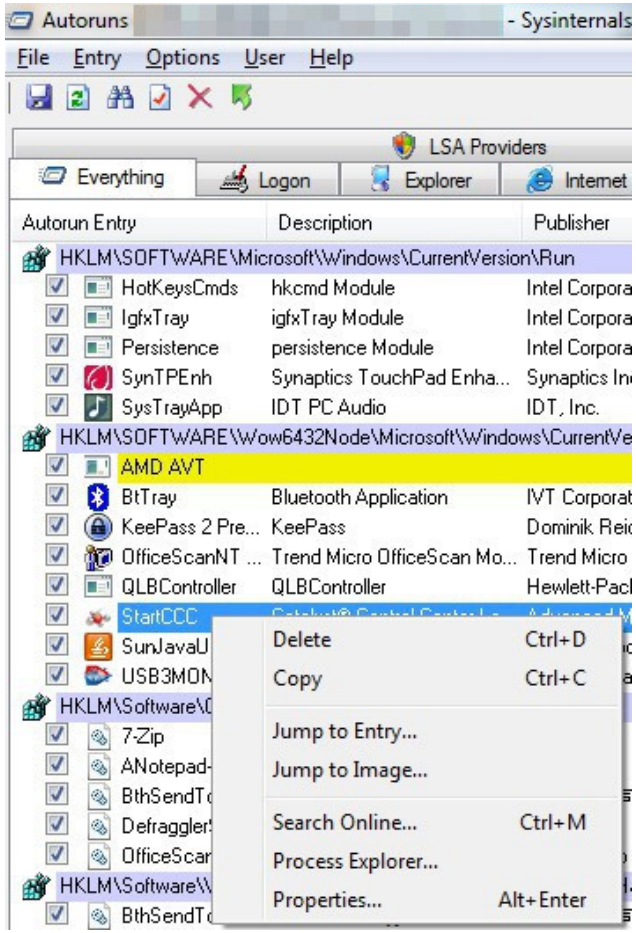


Actions sur une entrée

Delete Suppression de l'entrée

Copy Copie l'ensemble des informations lié à l'Entrée

Jump to Entry Ouvrir la localisation de l'Entrée



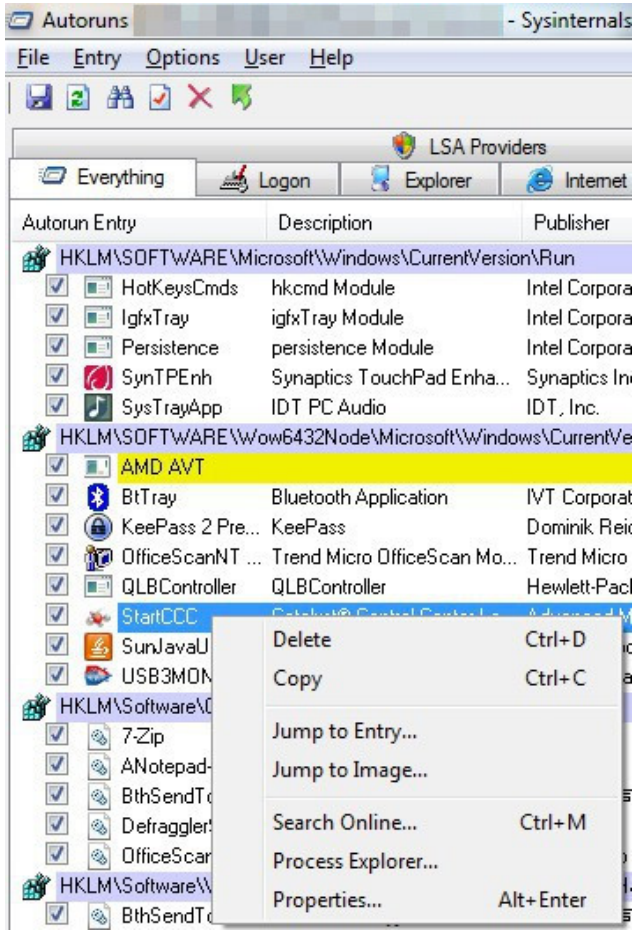
Actions sur une entrée

Delete Suppression de l'entrée

Copy Copie l'ensemble des informations lié à l'Entrée

Jump to Entry Ouvrir la localisation de l'Entrée

Jump to Image Ouvrir la localisation de l' ń Exécutable ż



Actions sur une entrée

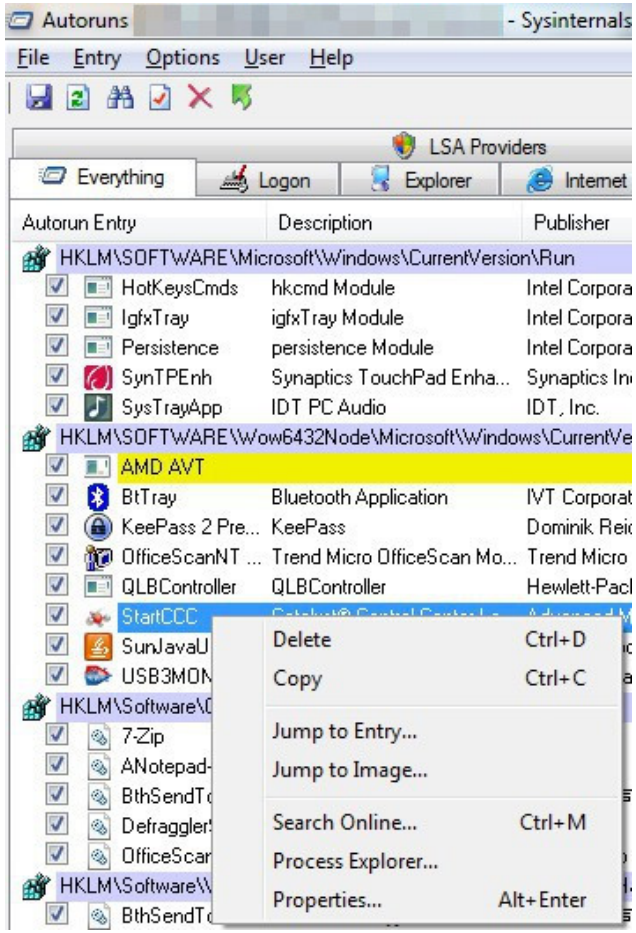
Delete Suppression de l'entrée

Copy Copie l'ensemble des informations lié à l'Entrée

Jump to Entry Ouvrir la localisation de l'Entrée

Jump to Image Ouvrir la localisation de l' ń Exécutable ż

Search Online Recherche d'informations sur Internet



Actions sur une entrée

Delete Suppression de l'entrée

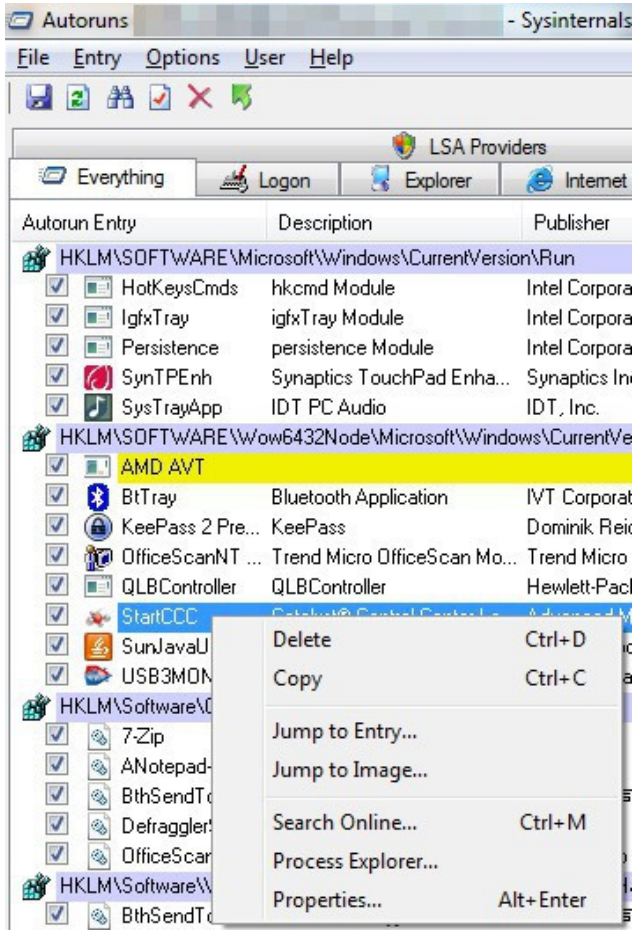
Copy Copie l'ensemble des informations lié à l'Entrée

Jump to Entry Ouvrir la localisation de l'Entrée

Jump to Image Ouvrir la localisation de l' ń Exécutable ż

Search Online Recherche d'informations sur Internet

Process Explorer Recherche le PID dans Process Explorer



Sauvegarde pour comparaison

- Autoruns ne peut pas nous indiquer l'état de votre système dans le passé. Par contre, il peut comparer ce que vous avez sauvegardé avec l'état actuel.

Sauvegarde pour comparaison

- Autoruns ne peut pas nous indiquer l'état de votre système dans le passé. Par contre, il peut comparer ce que vous avez sauvegardé avec l'état actuel.
- Pour sauvegarder une log Autoruns, File Save.

Sauvegarde pour comparaison

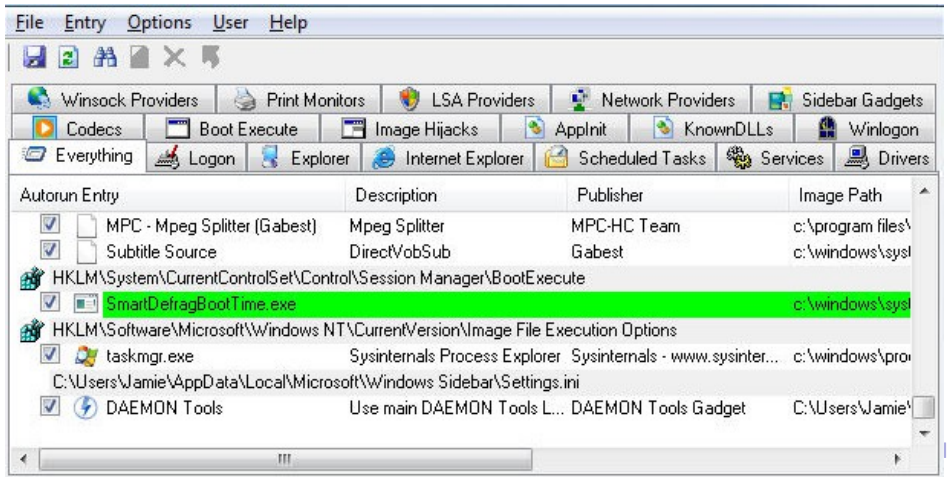
- Autoruns ne peut pas nous indiquer l'état de votre système dans le passé. Par contre, il peut comparer ce que vous avez sauvegardé avec l'état actuel.
- Pour sauvegarder une log Autoruns, File Save.
- Si vous désirez le comparer, `File - Compare` et ouvrez le fichier précédemment sauvegardé. Les différences apparaissent en VERT.

Sauvegarde pour comparaison

- Autoruns ne peut pas nous indiquer l'état de votre système dans le passé. Par contre, il peut comparer ce que vous avez sauvegardé avec l'état actuel.
- Pour sauvegarder une log Autoruns, File Save.
- Si vous désirez le comparer, `File - Compare` et ouvrez le fichier précédemment sauvegardé. Les différences apparaissent en VERT.

Sauvegarde pour comparaison

- Autoruns ne peut pas nous indiquer l'état de votre système dans le passé. Par contre, il peut comparer ce que vous avez sauvegardé avec l'état actuel.
- Pour sauvegarder une log Autoruns, File Save.
- Si vous désirez le comparer, `File - Compare` et ouvrez le fichier précédemment sauvegardé. Les différences apparaissent en VERT.

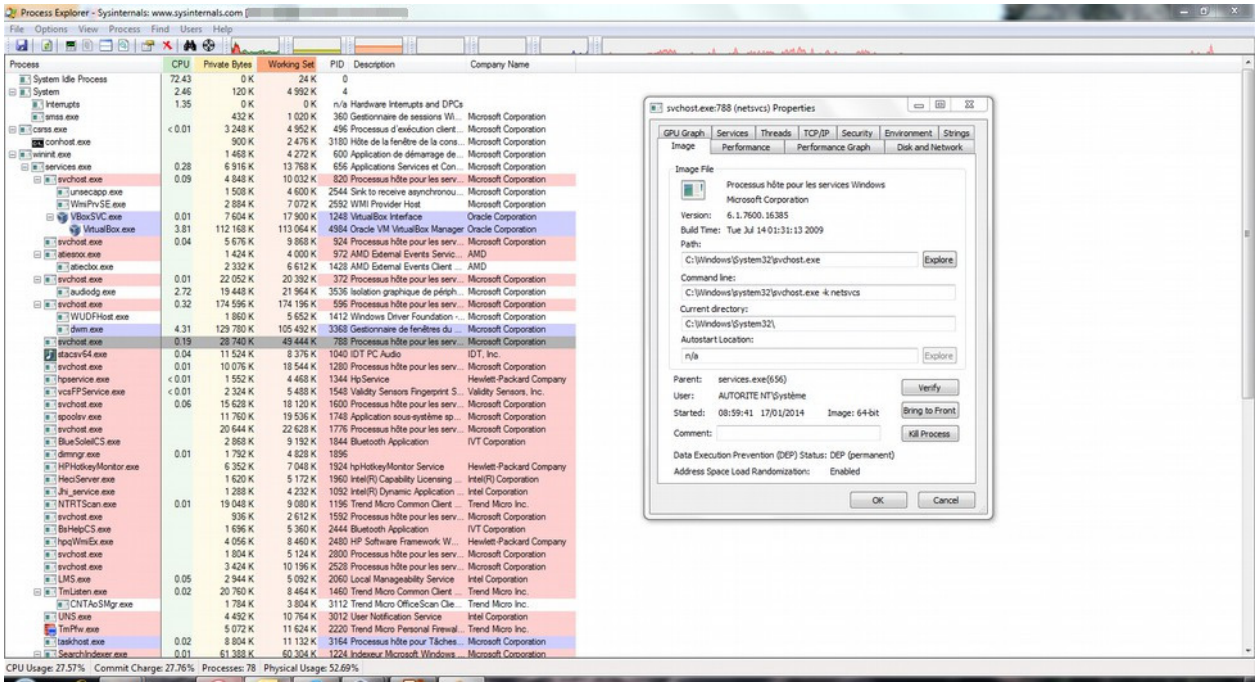


ProcessExplorer

ProcessExplorer est l'équivalent du Gestionnaire des Tâches en amélioré.

ProcessExplorer

ProcessExplorer est l'équivalent du Gestionnaire des Tâches en amélioré.



Les codes couleurs

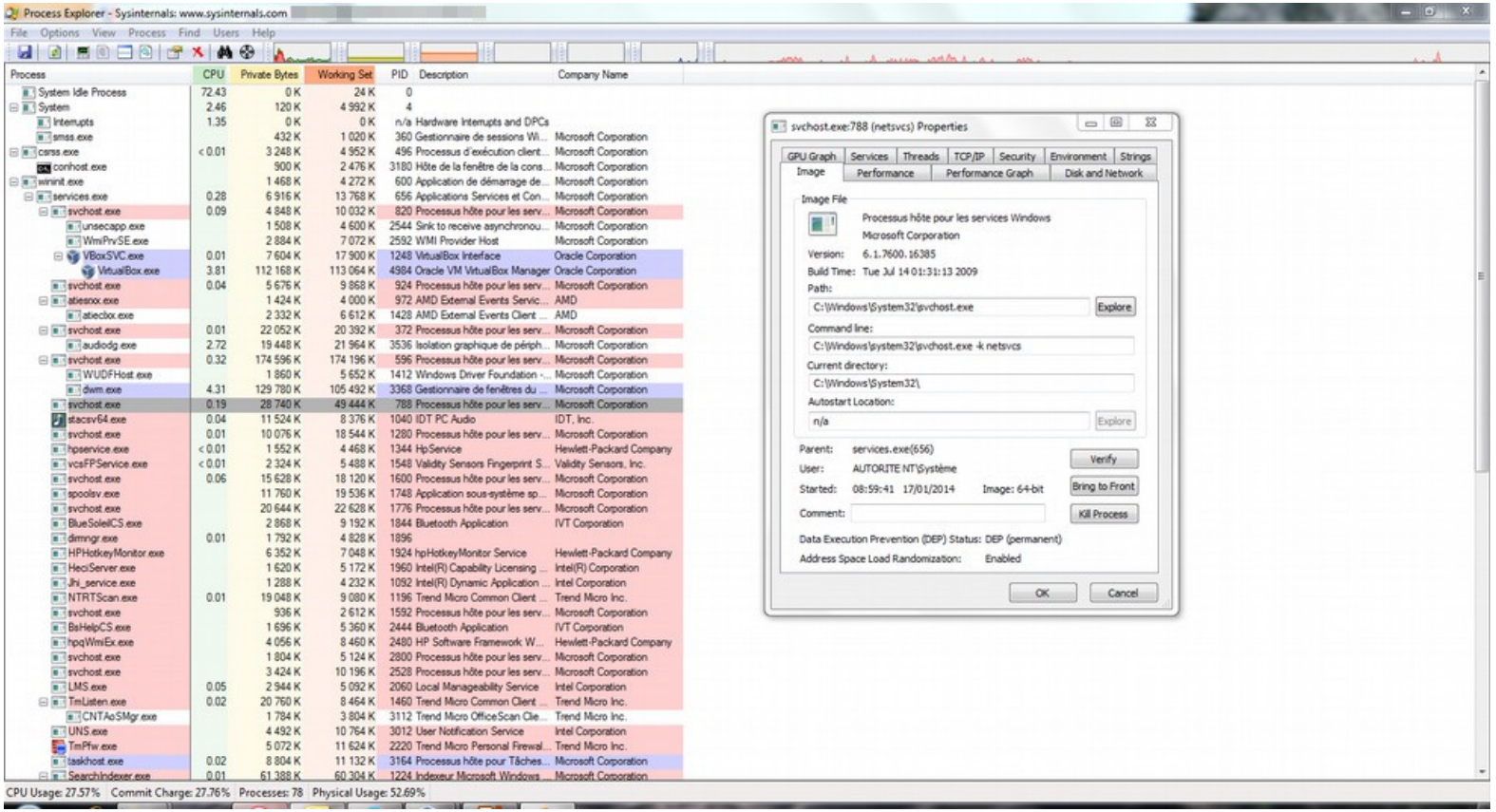
Bleu	Indique que le processus est en cours d'exécution dans le même contexte de sécurité que Process Explorer. Généralement, ceci indique qu'il s'exécute dans l'environnement de l'utilisateur plutôt que dans un environnement de service ou de système.
Rose	Indique que le processus est hébergé par un ou plusieurs services de Windows. Les services peuvent s'exécuter par eux même ou comme partie de services (DLL) au travers du processus `svchost.exe`.
Violet	Indique que l'image est obfusquée (compressée ou chiffrée).
Vert Rouge	Les couleurs Verte et Rouge indiquent que le processus vient juste respectivement de démarrer ou de s'arrêter.

Arbre

- Process Explorer conserve une trace de la relation Parent / Enfant
- Les processus orphelins sont justifiés à gauche.

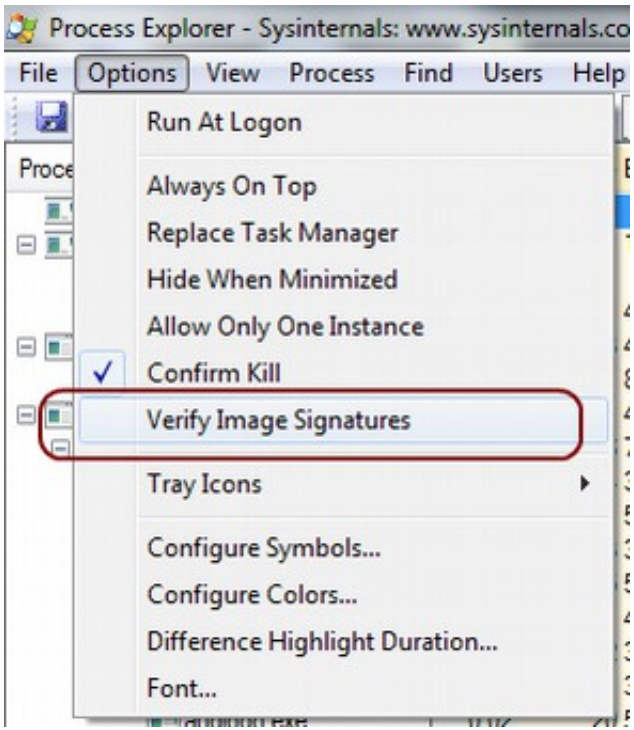
csrss.exe	0.22	2 876 K	90 016 K	624	Processus d'exécution client...	Microsoft Corporation
winlogon.exe		2 824 K	7 324 K	708	Application d'ouverture de s...	Microsoft Corporation
explorer.exe	0.12	69 980 K	91 748 K	1508	Explorateur Windows	Microsoft Corporation
igfxtray.exe		2 304 K	6 328 K	3412	igfxTray Module	Intel Corporation
hkcmd.exe		2 164 K	6 196 K	3628	hkcmd Module	Intel Corporation
igfxpers.exe		2 564 K	7 228 K	1388	persistence Module	Intel Corporation
sttray64.exe		8 420 K	18 988 K	3708	IDT PC Audio	IDT, Inc.
SynTPEnh.exe	< 0.01	8 704 K	12 864 K	3744	Synaptics TouchPad Enhan...	Synaptics Incorporated
OUTLOOK.EXE	0.21	105 212 K	189 812 K	4244	Microsoft Outlook	Microsoft Corporation
simpress.exe		796 K	2 824 K	4268	LibreOffice Impress	The Document Foundation
soffice.exe		1 020 K	3 200 K	4692	LibreOffice	The Document Foundation
soffice.bin	0.05	116 320 K	146 156 K	4276	LibreOffice	The Document Foundation
splwow64.exe		2 012 K	5 616 K	3300	Print driver host for 32bit appl...	Microsoft Corporation
firefox.exe	0.38	143 108 K	149 532 K	3408	Firefox	Mozilla Corporation
procexp.exe		2 336 K	7 336 K	3924	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	1.99	26 936 K	39 228 K	4600	Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	0.03	3 596 K	12 156 K	5688	Outil Capture	Microsoft Corporation
QLBController.exe		49 152 K	38 880 K	2688	QLBController	Hewlett-Packard Company
iusb3mon.exe		1 944 K	5 340 K	828	Intel(R) USB 3.0 Monitor	Intel Corporation
PccNTMon.exe	0.71	6 440 K	4 112 K	3284	Trend Micro OfficeScan Mon...	Trend Micro Inc.
SynTPHelper.exe		1 192 K	3 120 K	3292	Synaptics Pointing Device H...	Synaptics Incorporated
BtTray.exe		3 728 K	11 940 K	3476	Bluetooth Application	IVT Corporation
MOM.exe	0.01	40 044 K	5 356 K	4868	Catalyst Control Center: Moni...	Advanced Micro Devices I...
CCC.exe	< 0.01	99 760 K	4 960 K	4952	Catalyst Control Center: Host...	ATI Technologies Inc.
VirtualBox.exe	0.14	42 064 K	70 120 K	4332	Oracle VM VirtualBox Manager	Oracle Corporation

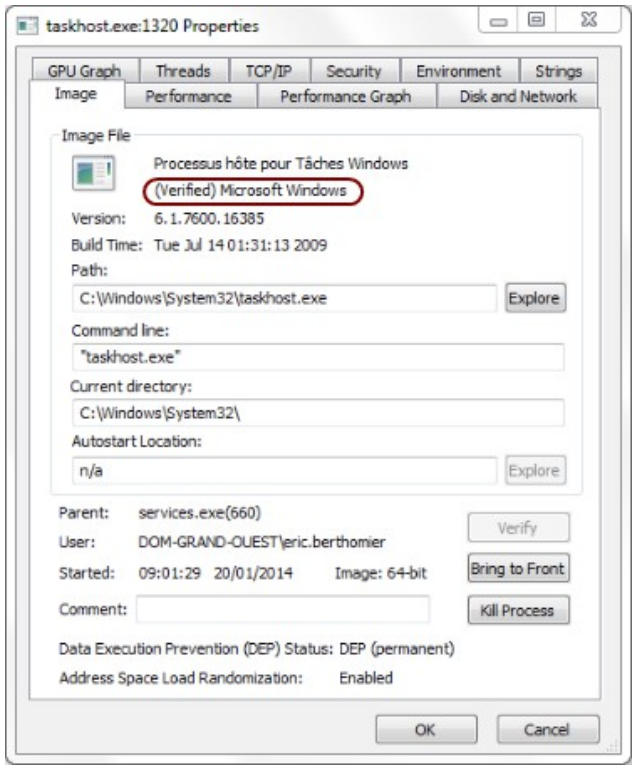
Propriétés d'un processus



Vérification de signature

L'ensemble des outils SysInternals permet de Vérifier la signature des fichiers.





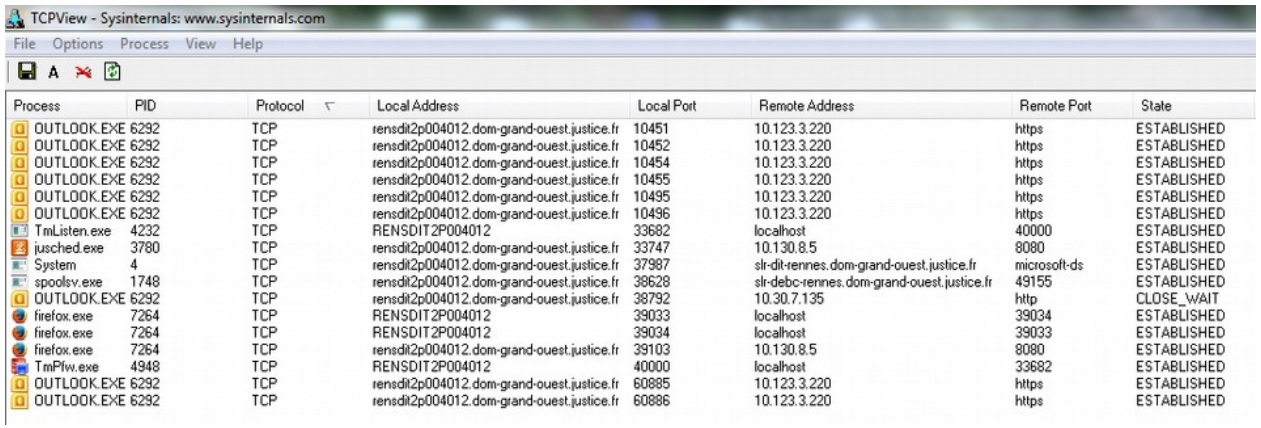
TcpView

TCPView est l'équivalent de la commande NETSTAT en amélioré.

TcpView

TCPView est l'équivalent de la commande NETSTAT en amélioré.
TCP View possède 2 ń grands ż modes :

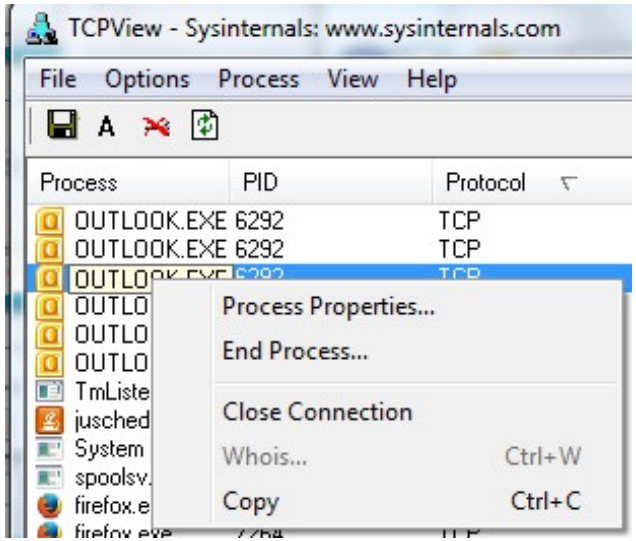
- Toutes les connexions (actives + inactives)
- Seules les connexions établies



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	10451	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	10452	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	10454	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	10455	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	10495	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	10496	10.123.3.220	https	ESTABLISHED
TmListen.exe	4232	TCP	RENSDIT2P004012	33682	localhost	40000	ESTABLISHED
jusched.exe	3780	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	33747	10.130.8.5	8080	ESTABLISHED
System	4	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	37987	slr-dit-rennes.dom-grand-ouest.justice.fr	microsoft-ds	ESTABLISHED
spoolsv.exe	1748	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	38628	slr-debc-rennes.dom-grand-ouest.justice.fr	49155	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	38792	10.30.7.135	http	CLOSE_WAIT
firefox.exe	7264	TCP	RENSDIT2P004012	39033	localhost	39034	ESTABLISHED
firefox.exe	7264	TCP	RENSDIT2P004012	39034	localhost	39033	ESTABLISHED
firefox.exe	7264	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	39103	10.130.8.5	8080	ESTABLISHED
TmPfw.exe	4948	TCP	RENSDIT2P004012	40000	localhost	33682	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	60885	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensdit2p004012.dom-grand-ouest.justice.fr	60886	10.123.3.220	https	ESTABLISHED

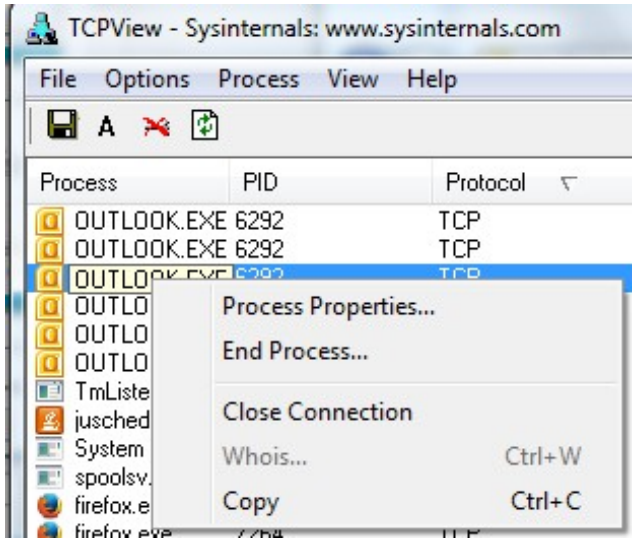
Utilisation (1/2)

- Les couleurs



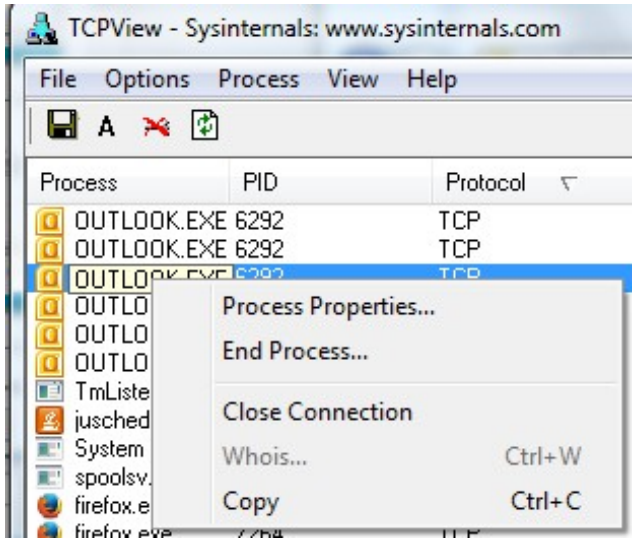
Utilisation (1/2)

- Les couleurs
  - Les connexions venant de se créer sont montrées en vert.



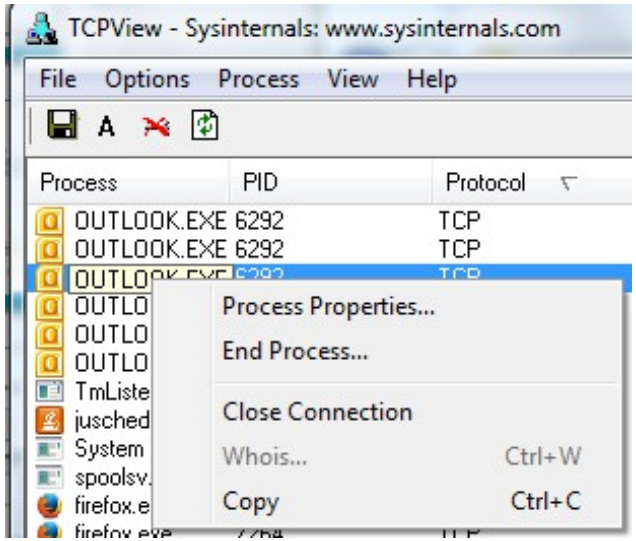
Utilisation (1/2)

- Les couleurs
  - Les connexions venant de se créer sont montrées en vert.
  - Les connexions changeant de serveur ou de port sont montrées en jaune.



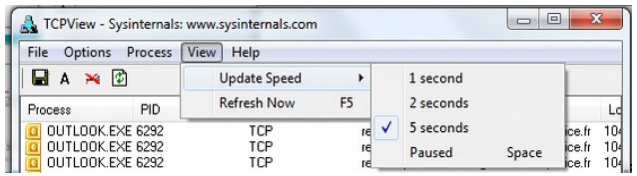
Utilisation (1/2)

- Les couleurs
  - Les connexions venant de se créer sont montrées en vert.
  - Les connexions changeant de serveur ou de port sont montrées en jaune.
  - Les connexions se fermant s'affichent en rouge.



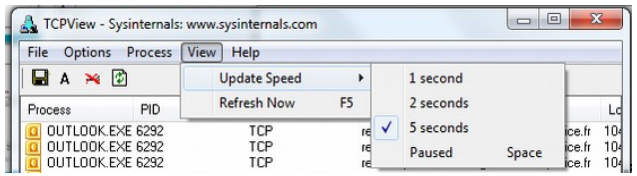
Utilisation (2/2)

- View Update Speed (Délai de mise à jour)



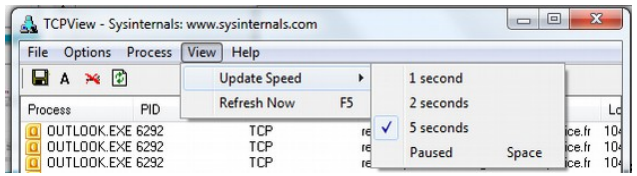
Utilisation (2/2)

- View Update Speed (Délai de mise à jour)
- Options : Resolve Adresses permet de voir le nom du serveur distant auquel vous êtes connecté plutôt que son IP.



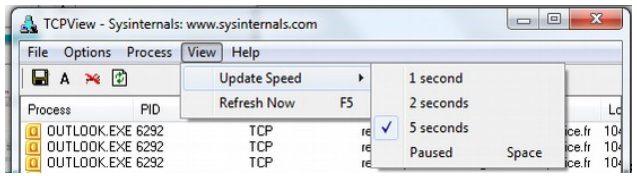
Utilisation (2/2)

- View Update Speed (Délai de mise à jour)
- Options : Resolve Adresses permet de voir le nom du serveur distant auquel vous êtes connecté plutôt que son IP.
- Clic droit sur une connexion :



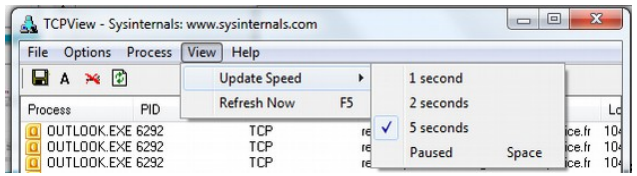
Utilisation (2/2)

- View Update Speed (Délai de mise à jour)
- Options : Resolve Adresses permet de voir le nom du serveur distant auquel vous êtes connecté plutôt que son IP.
- Clic droit sur une connexion :
  - Close Connection : Fermeture de la connexion réseau



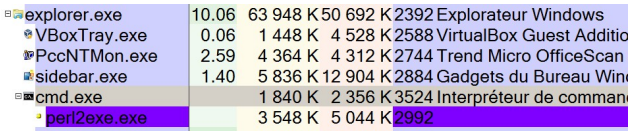
Utilisation (2/2)

- View Update Speed (Délai de mise à jour)
- Options : Resolve Adresses permet de voir le nom du serveur distant auquel vous êtes connecté plutôt que son IP.
- Clic droit sur une connexion :
  - Close Connection : Fermeture de la connexion réseau
  - End Process ... : Arrêt du processus associé à la connexion réseau



Code obfusqué

L'ensemble des outils SysInternals permet de pointer les codes obfusqués (impénétrables).
La couleur Violet foncée est utilisée pour montrer les fichiers suspicieux (obfusqué ou chiffré).



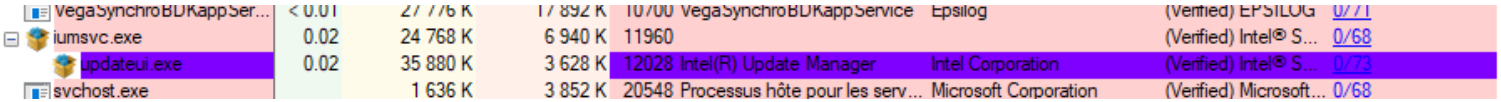
L'exécution de PERL2EXE sur un code offusqué déclenche une alerte dans SysInternals
`http://perlobfuscator.com/po.cgi`

Pourquoi un code obfusqué ?

Il est possible d'obfusquer son code pour principalement 3 raisons :

- Pour protéger son code (`http://www.phpencode.org/`)
- Pour s'amuser (`http://www0.us.ioccc.org/`)
- Pour éviter que l'on voit ce qu'il fait
  `http://www.brandonparker.net/code_obf.php/`

Exemple pour se protéger



Exemple malveillant

Des utilisateurs ont reçu par courriel un fichier zip contenant un bien étrange programme écrit en Visual Basic . . .

```
ExecuteGlobal(((((chr(((((  3150-3068  ))))) & chr(((((  2364-2267  ))))) & chr(((((  1093290/9939  ))
      ))) & chr(((((  8057-7957  ))))) & chr(((((  646242/5822  ))))) & chr(((((  3064-2955  ))))) &
      chr(((((  9415-9310  ))))) & chr(((((  105164/862  ))))) & chr(((((  913848/9048  )))))
```

Exemple malveillant

Des utilisateurs ont reçu par courriel un fichier zip contenant un bien étrange programme écrit en Visual Basic . . .

```
ExecuteGlobal(((((chr(((((  3150-3068 ))))) & chr(((((  2364-2267 ))))) & chr(((((  1093290/9939 ))
      ))) & chr(((((  8057-7957 ))))) & chr(((((  646242/5822 ))))) & chr(((((  3064-2955 ))))) &
      chr(((((  9415-9310 ))))) & chr(((((  105164/862 ))))) & chr(((((  913848/9048 )))))
```

ExecuteGlobal signifie : exécuter la résultante du contenu entre parenthèses. Chr renvoie la lettre correspondant au code Ascii renseigné.

3150 − 3068 = 82 : Lettre R 2364 − 2267 = 97 : Lettre a

. . .

Exemple malveillant

Des utilisateurs ont reçu par courriel un fichier zip contenant un bien étrange programme écrit en Visual Basic . . .

```
ExecuteGlobal(((((chr(((((  3150-3068 ))))) & chr(((((  2364-2267 ))))) & chr(((((  1093290/9939 ))
      ))) & chr(((((  8057-7957 ))))) & chr(((((  646242/5822 ))))) & chr(((((  3064-2955 ))))) &
      chr(((((  9415-9310 ))))) & chr(((((  105164/862 ))))) & chr(((((  913848/9048 )))))
```

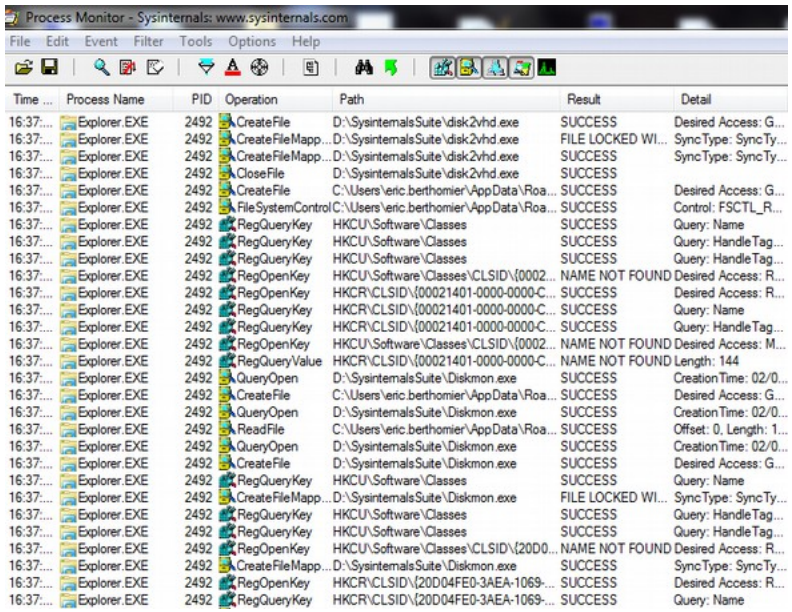
ExecuteGlobal signifie : exécuter la résultante du contenu entre parenthèses. Chr renvoie la lettre correspondant au code Ascii renseigné.

$3150 \;\; 3068 = 82$: Lettre R $\qquad$ $2364 \;\; 2267 = 97$: Lettre a

. . . Au final ce joli code signifie ń Randomize ż et permettait d'initialiser le processus de gestion de l'aléatoire afin de créer un fichier avec un nom non prédictible afin de mieux le maquiller.

ProcessMonitor : Procmon

Process Monitor permet d'explorer l'ensemble des appels systèmes effectués par un processus à tout moment.



Icon	Event
	Registry
	File System
	Network
	Process
	Profiling

Sources

- Analyze all Autorun / Auto-start programs in Windows
  `http://www.afterdawn.com/guides/archive/analyze_all_autorun_auto-start_programs_in_windows.cfm`
- Windows Internals and Advanced Troubleshooting [Solomon, Russinovich; 2002]
- Windows SysInternals Administrator's Reference