

SysInternals

Éric BERTHOMIER
eric.berthomier@free.fr

March 16, 2022



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



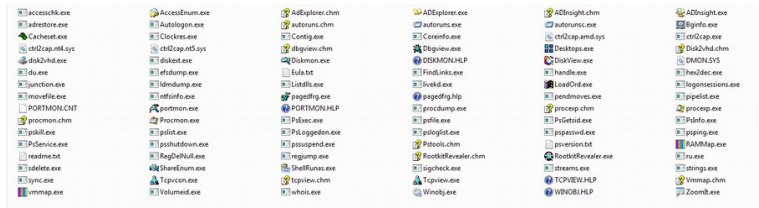
Présentation de la suite SysInternals

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



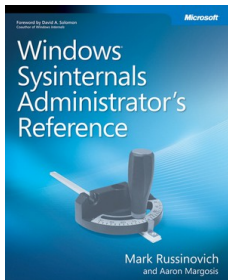
3 Outils parmi tant d'autres

- Autoruns
- ProcessExplorer
- TcpView



3 Outils parmi tant d'autres

- Autoruns
- ProcessExplorer
- TcpView



494 pages

Formation de 5 jours . . .



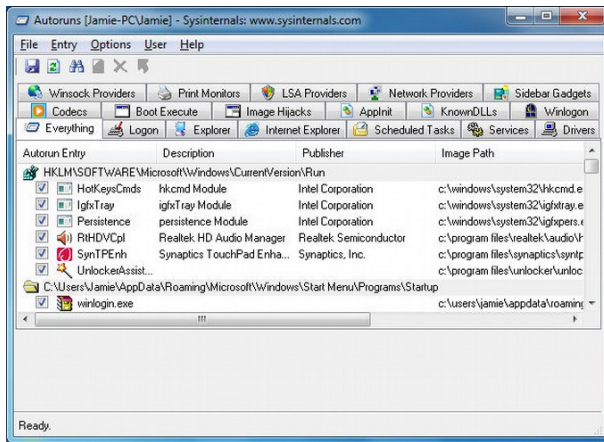
Autoruns

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 à l'état de démarrage 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 à l'état de démarrage 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 :

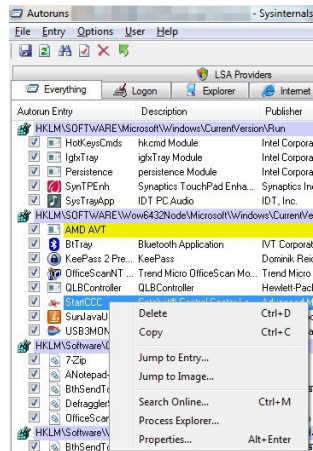
- Pour chaque élément, le
 - Désactiver
 - Supprimer
 - Analyser
- D'enregistrer à l'état de démarrage à un instant t pour le comparer par la suite

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.

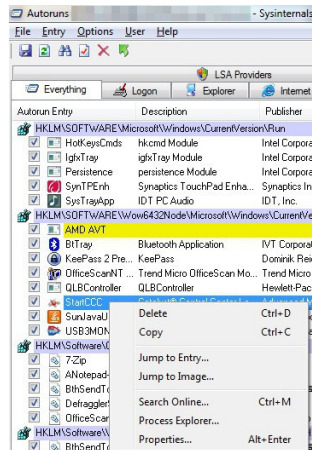
Actions sur une entrée

Delete Suppression de l'entrée



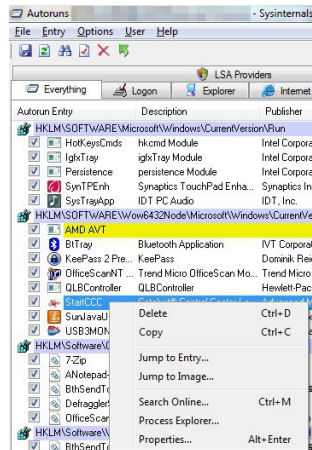
Actions sur une entrée

- 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



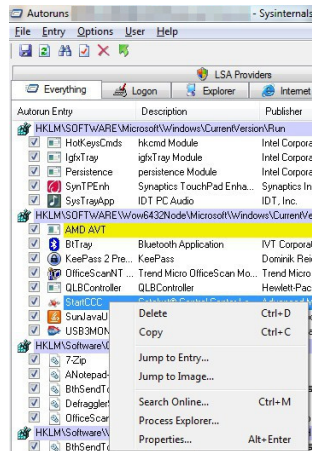
Actions sur une entrée

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'Exécutable



Actions sur une entrée

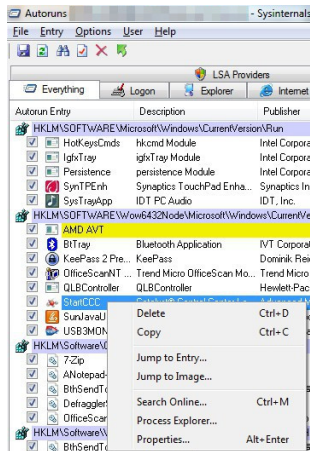
Delete Suppression de l'entrée

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'Exécutable

Search Online Recherche d'informations sur Internet



Actions sur une entrée

Delete Suppression de l'entrée

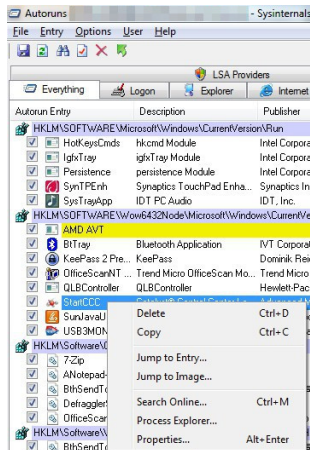
Copy Copie l'ensemble des informations lié à l'Entrée

Jump to Entry Ouvrir la localisation de l'Entrée

Jump to Image Ouvrir la localisation de l'Exécutable

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.



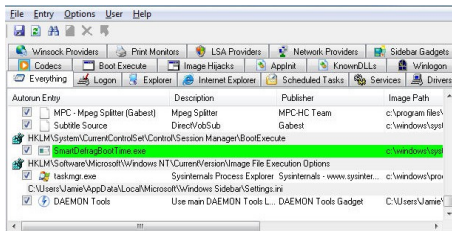
Sauvegarde pour comparaison

- 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.



[illegible]

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 <code>svchost.exe</code> .
Violet	Indique que l'image est obfusquée (compressée ou chiffrée).
Vert	Les couleurs Verte et Rouge indiquent que le processus vient juste respectivement de démarrer ou de s'arrêter.
Rouge	



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
igbttray.exe		2 304 K	6 328 K	3412 igbtTray 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 Enhanc...	Synaptics Incorporated
OUTLOOK.EXE	0.21	105 212 K	189 812 K	4244 Microsoft Outlook	Microsoft Corporation
simpres.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...
Snipping Tool.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
usb3mon.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
BluetoothTray.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

The screenshot shows the Process Explorer application with a list of processes. The 'svchost.exe' process is highlighted. A properties window for 'svchost.exe (netvcs)' is open, displaying various details about the process.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	72.43	0 K	24 K	0		
System	2.46	120 K	4	4		
smss.exe	1.35	0 K	0 K	n/a	Hardware Interrupts and DPCs	
csrss.exe	432 K	1 020 K	360	Gestionnaire de sessions W...	Microsoft Corporation	
smss.exe	3.248 K	4 952 K	496	Processus d'installation client...	Microsoft Corporation	
csrss.exe	900 K	2 476 K	3180	Hôte de la fenêtre de la cons...	Microsoft Corporation	
smss.exe	1 468 K	4 272 K	600	Application de démarrage de...	Microsoft Corporation	
csrss.exe	5 916 K	13 768 K	656	Applications Services et Con...	Microsoft Corporation	
svchost.exe	0.28	4 848 K	10 032 K	820	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	0.09	1 508 K	4 600 K	2544	Service à recevoir asynchron...	Microsoft Corporation
svchost.exe	0.01	2 884 K	7 072 K	20932	VMW Provider Host	Microsoft Corporation
svchost.exe	0.01	7 604 K	17 900 K	1248	VirtualBox interface	Oracle Corporation
svchost.exe	3.81	112 168 K	113 064 K	4804	Oracle VM VirtualBox Manager	Oracle Corporation
svchost.exe	0.04	5 076 K	9 988 K	324	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	1.424 K	3 972 K	4 000 K	972	AMD External Events Serv...	AMD
svchost.exe	2.322 K	6 612 K	1 423	AMD External Events Client	AMD	
svchost.exe	0.01	22 002 K	20 302 K	372	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	2.72	19 448 K	21 964 K	3536	Isolation graphique de périph...	Microsoft Corporation
svchost.exe	0.32	174 596 K	174 196 K	596	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	0.11	1 860 K	6 652 K	1 412	Windows Driver Foundation	Microsoft Corporation
svchost.exe	4.31	129 780 K	105 492 K	3368	Gestionnaire de fenêtres du...	Microsoft Corporation
svchost.exe	0.19	28 740 K	49 444 K	788	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	0.04	11 524 K	6 178 K	1340	OT PC Audio	OTI, Inc.
svchost.exe	0.01	10 076 K	18 544 K	1280	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	0.01	1 552 K	4 468 K	1344	hp Service	Hewlett-Packard Company
svchost.exe	0.01	2 324 K	5 438 K	1548	Validity Sensors Fingerprint S...	Validity Sensors, Inc.
svchost.exe	0.06	15 628 K	18 120 K	1600	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	11 760 K	19 536 K	1 743	Application sous-système op...	Microsoft Corporation	
svchost.exe	20 644 K	22 528 K	1 776	Processus hôte pour les serv...	Microsoft Corporation	
svchost.exe	2 888 K	9 192 K	1 844	Bluetooth Application	IVT Corporation	
svchost.exe	0.01	1 792 K	4 628 K	1 896		
svchost.exe	0.01	6 262 K	7 048 K	1824	hpGatewayMonitor Service	Hewlett-Packard Company
svchost.exe	1 620 K	5 172 K	1 960	Intel(R) Capability Licensing...	Intel(R) Corporation	
svchost.exe	1 288 K	4 232 K	1 952	Intel(R) Dynamic Application	Intel Corporation	
svchost.exe	19 048 K	9 080 K	1 196	Trend Micro Common Client	Trend Micro Inc.	
svchost.exe	936 K	2 612 K	1 592	Processus hôte pour les serv...	Microsoft Corporation	
svchost.exe	1 696 K	5 260 K	2 444	Bluetooth Application	IVT Corporation	
svchost.exe	4 096 K	8 402 K	2480	WP Software Framework W...	Hewlett-Packard Company	
svchost.exe	1 804 K	5 124 K	2 800	Processus hôte pour les serv...	Microsoft Corporation	
svchost.exe	2 424 K	10 196 K	2528	Processus hôte pour les serv...	Microsoft Corporation	
svchost.exe	2 944 K	5 092 K	2 060	Local Manageability Service	Intel Corporation	
svchost.exe	0.05	20 760 K	8 464 K	1 460	Trend Micro Common Client	Trend Micro Inc.
svchost.exe	0.02	1 784 K	3 804 K	3 112	Trend Micro OfficeScan Cl...	Trend Micro Inc.
svchost.exe	4 482 K	10 764 K	3 012	User Notification Service	Intel Corporation	
svchost.exe	5 072 K	11 624 K	2 220	Trend Micro Personal Firewall	Trend Micro Inc.	
svchost.exe	0.02	8 804 K	11 132 K	3 164	Processus hôte pour les serv...	Microsoft Corporation
svchost.exe	0.01	61 388 K	60 364 K	1 224	Indexeur Microsoft Windows...	Microsoft Corporation

svchost.exe (netvcs) Properties

Image File: C:\Windows\System32\svchost.exe

Version: 6.1.7600.16385

Build Time: Tue Jul 14 01:31:13 2009

Path: C:\Windows\System32\svchost.exe

Command line: C:\Windows\System32\svchost.exe -k netvcs

Current directory: C:\Windows\System32\

Autostart Location: n/a

Parent: services.exe (596)

User: AUTHENTICATED SYSTEM

Started: 08:59:41 1/27/2014 Image: 64-bit

Comment:

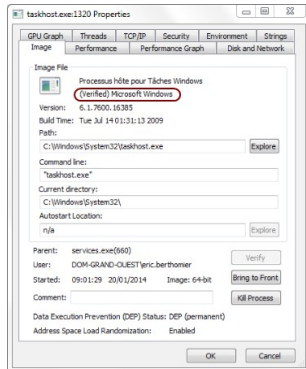
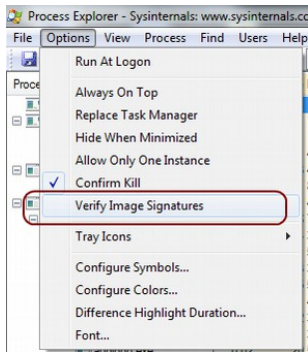
Data Execution Prevention (DEP) Status: DEP (Optimant)

Address Space Load Randomization: Enabled

CPU Usage: 27.36% Committ Charge: 27.36% Processes: 78 Physical Usage: 52.69%

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 grands modes :

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



TCPView - Sysinternals: www.sysinternals.com

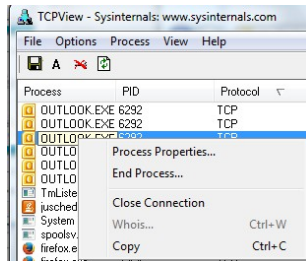
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	10451	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	10452	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	10453	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	10454	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	10455	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	10456	10.123.3.220	https	ESTABLISHED
Telnet.exe	4232	TCP	rensi2p004012	23882	localhost	40000	ESTABLISHED
rsched.exe	3780	TCP	rensi2p004012.dom-grand-ouest.justice.fr	33747	10.130.8.5	8080	ESTABLISHED
System	4	TCP	rensi2p004012.dom-grand-ouest.justice.fr	37987	sk-dit-rennes.dom-grand-ouest.justice.fr	49155	ESTABLISHED
spoolsv.exe	1748	TCP	rensi2p004012.dom-grand-ouest.justice.fr	38628	sk-debo-rennes.dom-grand-ouest.justice.fr	49155	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	38792	10.30.7.135	http	CLOSE_WAIT
firefox.exe	7264	TCP	rensi2p004012	29033	localhost	39034	ESTABLISHED
firefox.exe	7264	TCP	rensi2p004012	29034	localhost	39033	ESTABLISHED
firefox.exe	7264	TCP	rensi2p004012.dom-grand-ouest.justice.fr	29103	10.130.8.5	8080	ESTABLISHED
TcpView.exe	4948	TCP	rensi2p004012	40000	localhost	33882	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	60895	10.123.3.220	https	ESTABLISHED
OUTLOOK.EXE	6292	TCP	rensi2p004012.dom-grand-ouest.justice.fr	60896	10.123.3.220	https	ESTABLISHED



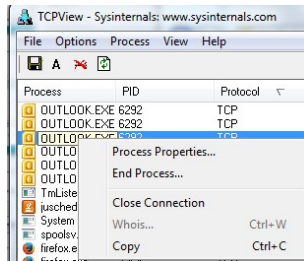
Utilisation (1/2)

- Les couleurs



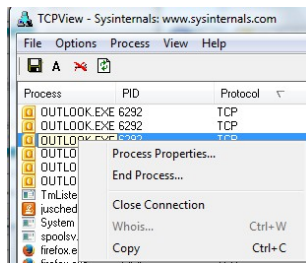
Utilisation (1/2)

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



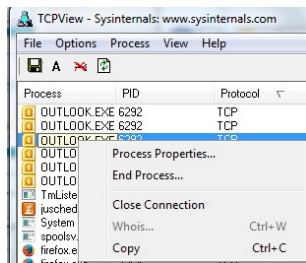
Utilisation (1/2)

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



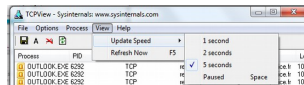
Utilisation (1/2)

- 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.



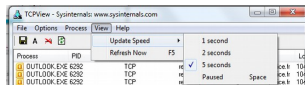
Utilisation (2/2)

- View Update Speed (Délai de mise à jour)



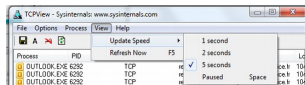
Utilisation (2/2)

- 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.



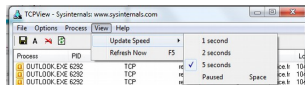
Utilisation (2/2)

- 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 :



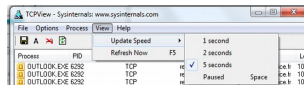
Utilisation (2/2)

- 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 suspects (obfusqué ou chiffré).

explorer.exe	10.06	63 948 K	50 692 K	2392	Explorateur Windows
VBoxTray.exe	0.06	1 448 K	4 528 K	2588	VirtualBox Guest Additio
PccNTMon.exe	2.59	4 364 K	4 312 K	2744	Trend Micro OfficeScan
sidebar.exe	1.40	5 836 K	12 904 K	2884	Gadgets du Bureau Win
cmd.exe	1.840	K	2 356 K	3524	Interpréteur de comman
perl2exe.exe	3.548	K	5 044 K	2992	

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/

```

1  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000

```



Exemple pour se protéger

vegasyndroBUKappser...	< 0.01	27 776 K	17 892 K	10/100	VegasyndroBUKappService - Epsilog	(Verified) EPSILOG	0/71
umsvc.exe	0.02	24 768 K	6 940 K	11960		(Verified) Intel® S...	0/68
updateui.exe	0.02	35 880 K	3 628 K	12028	Intel(R) Update Manager - Intel Corporation	(Verified) Intel® S...	0/77
svchost.exe		1 636 K	3 852 K	20548	Processus hôte pour les serv... - Microsoft Corporation	(Verified) Microsoft...	0/68



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.

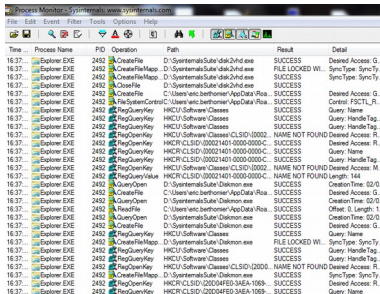
3150 3068 = 82 : Lettre R 2364 2267 = 97 : Lettre a

... Au final ce joli code signifie `Randomize` 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.



Time	Process Name	PID	Operation	Path	Result	Detail
16:37	Explorer.EXE	2452	CreateFile	D:\System32\subsystem.exe	SUCCESS	Desired Access: G...
16:37	Explorer.EXE	2452	CreateFileMap	D:\System32\subsystem.exe	FILE LOCKED W...	SyncType: SyncTy...
16:37	Explorer.EXE	2452	CreateFileMap	D:\System32\subsystem.exe	SUCCESS	SyncType: SyncTy...
16:37	Explorer.EXE	2452	CloseFile	D:\System32\subsystem.exe	SUCCESS	
16:37	Explorer.EXE	2452	CreateFile	C:\Users\eric.berthomier\AppData\Roa...	SUCCESS	Desired Access: G...
16:37	Explorer.EXE	2452	FileSystemControl	C:\Users\eric.berthomier\AppData\Roa...	SUCCESS	Control: FSCTL_R...
16:37	Explorer.EXE	2452	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:37	Explorer.EXE	2452	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
16:37	Explorer.EXE	2452	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: R...
16:37	Explorer.EXE	2452	RegOpenKey	HKCR\CLSID\{00021401-0000-0000-C...	SUCCESS	Desired Access: R...
16:37	Explorer.EXE	2452	RegQueryKey	HKCR\CLSID\{00021401-0000-0000-C...	SUCCESS	Query: Name
16:37	Explorer.EXE	2452	RegQueryKey	HKCR\CLSID\{00021401-0000-0000-C...	SUCCESS	Query: HandleTag...
16:37	Explorer.EXE	2452	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: R...
16:37	Explorer.EXE	2452	RegQueryValue	HKCR\CLSID\{00021401-0000-0000-C...	NAME NOT FOUND	Length: 144
16:37	Explorer.EXE	2452	QueryOpen	D:\System32\subsystem.exe	SUCCESS	CreationTime: 02/0...
16:37	Explorer.EXE	2452	CreateFile	C:\Users\eric.berthomier\AppData\Roa...	SUCCESS	Desired Access: G...
16:37	Explorer.EXE	2452	QueryOpen	D:\System32\subsystem.exe	SUCCESS	CreationTime: 02/0...
16:37	Explorer.EXE	2452	ReadFile	C:\Users\eric.berthomier\AppData\Roa...	SUCCESS	Offset: 0, Length: 1...
16:37	Explorer.EXE	2452	QueryOpen	D:\System32\subsystem.exe	SUCCESS	CreationTime: 02/0...
16:37	Explorer.EXE	2452	CreateFile	D:\System32\subsystem.exe	SUCCESS	Desired Access: G...
16:37	Explorer.EXE	2452	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:37	Explorer.EXE	2452	CreateFileMap	D:\System32\subsystem.exe	FILE LOCKED W...	SyncType: SyncTy...
16:37	Explorer.EXE	2452	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
16:37	Explorer.EXE	2452	RegOpenKey	HKCU\Software\Classes\CLSID\{0002...	NAME NOT FOUND	Desired Access: R...
16:37	Explorer.EXE	2452	CreateFileMap	D:\System32\subsystem.exe	SUCCESS	SyncType: SyncTy...
16:37	Explorer.EXE	2452	RegOpenKey	HKCR\CLSID\{20004FED-3AEE-10B9...	SUCCESS	Desired Access: R...
16:37	Explorer.EXE	2452	RegQueryKey	HKCR\CLSID\{20004FED-3AEE-10B9...	SUCCESS	Query: Name

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

