

Spis treści

<i>Przedmowa</i>	xix
<i>Wstęp</i>	xxi
<i>O autorach</i>	xxxii

Część I: Zaczynamy

1 Wprowadzenie do narzędzi Sysinternals	3
Przegląd narzędzi	4
Witryna Windows Sysinternals	8
Pobieranie narzędzi	9
Uruchamianie narzędzi bezpośrednio z sieci Web	12
Pojedynczy obraz wykonywalny	13
Forum Windows Sysinternals	14
Blog Windows Sysinternals	15
Blog Marka	15
Webcasty	16
Informacje licencyjne Sysinternals	16
End User License Agreement i przełącznik /accepteula	16
Często zadawane pytania na temat licencjonowania Sysinternals.	17
2 Kluczowe koncepcje systemu Windows	19
Prawa administracyjne	20
Procesy, wątki i zadania	24
Tryb użytkownika i tryb jądra	25
Dojścia	27
Izolacja aplikacji	28
Kontenery aplikacji	29
Procesy chronione	35
Stosy wywołań i symbole	37
Czym jest stos wywołań?	37
Czym są symbole?	39
Konfigurowanie symboli	41
Sesje, stacje okien, pulpity i komunikaty okien	43

Sesje usług pulpitu zdalnego	44
Stacje okien	46
Pulpity	47
Komunikaty okien	48

Część II: Podręcznik użytkownika

3 Process Explorer	53
Ogólny przegląd Procexp	54
Mierzenie zużycia procesora	56
Prawa administracyjne	57
Okno główne	58
Lista procesów	58
Dostosowywanie wyboru kolumn	71
Zapisywanie wyświetlanych danych	86
Pasek narzędzi	86
Identyfikowanie procesu-właściciela okna	88
Pasek stanu	89
Biblioteki DLL i dojścia	90
Odszukiwanie DLL-i lub dojść	91
Widok DLL	92
Widok Handle	97
Szczegóły procesu	102
Karta Image	102
Karta Performance	105
Karta Performance Graph	106
Karta GPU Graph	107
Karta Threads	108
Karta TCP/IP	108
Karta Security	109
Karta Environment	111
Karta Strings	112
Karta Services	113
Karta .NET	114
Karta Job	116
Szczegóły wątku	117
Weryfikowanie podpisów obrazów	120
Analiza VirusTotal	121

Informacje systemowe	123
Karta CPU	124
Karta Memory.....	125
Karta I/O	127
Karta GPU	128
Opcje wyświetlania	130
Procexp jako zamiennik Task Manager	131
Tworzenie procesów w narzędziu Procexp	132
Sesje innych użytkowników	132
Różne funkcjonalności	133
Opcje zamykania	133
Przełączniki wiersza polecenia	133
Przywracanie domyślnych ustawień Procexp	133
Zestawienie skrótów klawiszowych	134
4 Autoruns.....	135
Podstawy Autoruns.....	138
Wyłączanie lub usuwanie wpisów autostartu	140
Autoruns i uprawnienia administracyjne	140
Weryfikowanie podpisów kodu	141
Analiza VirusTotal	142
Ukrywanie wpisów	143
Uzyskiwanie dodatkowych informacji o wpisie.....	146
Wyświetlanie autostartów dla innych użytkowników.....	147
Przeglądanie lokalizacji ASEP systemu offline.....	147
Zmienianie fontu	148
Kategorie autostartu.....	148
Logon	148
Explorer	151
Internet Explorer.....	154
Scheduled Tasks	155
Services	155
Drivers	156
Codecs	157
Boot Execute.....	158
Image Hijacks	158
Applnit	160
KnownDLLs	161

Winlogon	161
Dostawcy Winsock	162
Print Monitors	163
LSA Providers	164
Network Providers	164
WMI	164
Sidebar Gadgets	165
Office	165
Zapisywanie i porównywanie wyników	166
Zapisywanie jako tekst rozdzielany tabulatorami	166
Zapisywanie w formacie binarnym (.arn)	167
Przeglądanie i porównywanie zapisanych wyników	167
AutorunsC	168
Autoruns i malware	171
5 Process Monitor	173
Podstawy Procmon	175
Zdarzenia	176
Domyślne ustawienia wyświetlanych kolumn	177
Dostosowywanie wyświetlanych kolumn	182
Okno dialogowe Event Properties	184
Wyświetlanie zdarzeń profilowania	189
Wyszukiwanie zdarzeń	191
Kopiowanie danych zdarzenia	191
Przechodzenie do lokalizacji pliku lub klucza rejestru	192
Wyszukiwanie online	192
Filtrowanie, wyróżnianie i zakładki	193
Konfigurowanie filtrów	193
Konfigurowanie wyróżniania	197
Zakładki	197
Zaawansowane wyjście	198
Zapisywanie filtrów do późniejszego użycia	199
Process Tree	201
Zapisywanie i otwieranie śladów Procmon	202
Zapisywanie śladów Procmon	203
Schemat XML programu Procmon	205
Otwieranie zapisanych śladów Procmon	208
Rejestrowanie aktywności rozruchu, logowania i zamykania	209

Rejestrowanie rozruchu	209
Utrzymanie działającego programu po wylogowaniu	211
Długo działające śledzenie i kontrolowanie wielkości dzinników	213
Odrzucanie filtrowanych zdarzeń	213
Głębokość historii	213
Pliki pomocnicze	214
Importowanie i eksportowanie ustawień konfiguracyjnych	215
Automatyzowanie Procmon: opcje wiersza polecenia	216
Narzędzia analizy	219
Process Activity Summary	220
File Summary	221
Registry Summary	223
Stack Summary	224
Network Summary	225
Cross Reference Summary	225
Count Occurrences	226
Wstawianie niestandardowego wyjścia debugowania do śladów	227
Pasek narzędzi	229
6 ProcDump	231
Składnia wiersza polecenia	233
Wskazywanie procesu do monitorowania	237
Dołączanie do istniejącego procesu	237
Uruchamianie docelowego procesu	238
Praca z aplikacjami Universal Windows Platform	239
Automatyczne debugowanie przy użyciu rejestracji AeDebug	241
Specyfikowanie ścieżki pliku rzutu	242
Określanie kryteriów dla rzutu	244
Monitorowanie wyjątków	249
Opcje plików rzutu	251
Rzuty Miniplus	254
ProcDump i Procmon: lepiej wspólnie	255
Nieinteraktywne uruchamianie ProcDump	258
Przeglądanie rzutu w debuggerze	259
7 PsTools	261
Wspólne funkcjonalności	262
Zdalne operacje	263

Rozwiązywanie problemów ze zdalnymi połączeniami PsTools.....	265
PsExec	267
Zakończenie zdalnego procesu	268
Przekierowane wyjście konsoli	269
Alternatywne poświadczenia PsExec	270
Opcje wiersza polecenia PsExec	271
Opcje wydajności procesu	272
Opcje łączności zdalnej	273
Opcje środowiska wykonywania	273
PsFile	277
PsGetSid	278
PsInfo	281
PsKill	283
PsList	284
PsLoggedOn	286
PsLogList	287
PsPasswd	292
PsService	293
Query	294
Config	296
Depend	297
Security	297
Find	298
SetConfig	299
Start, Stop, Restart, Pause, Continue	299
PsShutdown	299
PsSuspend	303
Składnia wiersza polecenia narzędzi PsTools	303
PsExec	304
PsFile	304
PsGetSid	304
PsInfo	304
PsKill	304
PsList	304
PsLoggedOn	304
PsLogList	304
PsPasswd	305
PsService	305

PsShutdown.....	305
PsSuspend.....	305
Wymagania systemowe PsTools.....	306
8 Narzędzia procesów i diagnostyki.....	307
VMMap.....	307
Uruchamianie VMMap i wybieranie procesu.....	309
Okno główne VMMap.....	311
Typy pamięci.....	313
Informacje o pamięci.....	314
Przebieg czasowy i migawki.....	316
Przeglądanie tekstu w regionach pamięci.....	318
Wyszukiwanie i kopiowanie tekstu.....	319
Wyświetlanie alokacji z procesów zinstrumentowanych.....	319
Fragmentacja przestrzeni adresowej.....	323
Zapisywanie i ładowanie wyników (migawek).....	323
Opcje wiersza polecenia VMMap.....	324
Przywracanie domyślnych ustawień VMMap.....	325
DebugView.....	325
Czym jest wyjście debugowania?.....	325
Okno DebugView.....	326
Przechwytywanie wyjścia debugowania trybu użytkownika.....	329
Przechwytywanie wyjścia debugowania trybu jądra.....	329
Wyszukiwanie, filtrowanie i wyróżnianie wyjścia.....	331
Zapisywanie, rejestrowanie i drukowanie.....	334
Monitorowanie zdalne.....	336
LiveKd.....	338
Wymagania LiveKd.....	339
Uruchamianie LiveKd.....	340
Typy celów debuggerów jądra.....	341
Wyjście do debugera lub pliku zrzutu.....	342
Zawartość zrzutu.....	343
Debugowanie systemów gości Hyper-V.....	345
Symbole.....	345
Przykłady użycia LiveKd.....	346
ListDLLs.....	348
Handle.....	351
Wyliczanie i wyszukiwanie dojść.....	352

Liczenie dojsć	355
Zamykanie dojsć	356
9 Narzędzia zabezpieczeń	357
SigCheck	358
Które pliki skanować	362
Weryfikacja podpisu	363
Analiza VirusTotal	365
Dodatkowe informacje o pliku	367
Format wyjścia	370
Różne	371
AccessChk	372
Czym są „efektywne uprawnienia”?	372
Korzystanie z AccessChk	373
Typ obiektu	376
Wyszukiwanie praw dostępu	380
Opcje wyjścia	381
Sysmon	384
Zdarzenia rejestrowane przez Sysmon	385
Instalowanie i konfigurowanie Sysmon	393
Wydobywanie danych zdarzeń Sysmon	399
AccessEnum	401
ShareEnum	403
ShellRunAs	405
Autologon	407
LogonSessions	408
SDelete	411
Korzystanie z SDelete	412
Jak działa SDelete	413
10 Narzędzia Active Directory	415
AdExplorer	415
Łączenie się z domeną	416
Okno AdExplorer	417
Obiekty	418
Atrybuty	419
Wyszukiwanie	421
Migawki	422

Konfiguracja AdExplorer	424
AdInsight	424
Przechwytywanie danych przez AdInsight	425
Opcje wyświetlania	429
Wyszukiwanie interesujących nas informacji	430
Filtrowanie wyników	432
Zapisywanie i eksportowanie danych AdInsight	434
Opcje wiersza polecenia	435
AdRestore	435
11 Narzędzia pulpitu	437
BglInfo	437
Konfigurowanie danych do wyświetlenia	438
Opcje wyglądu	442
Zapisywanie konfiguracji BglInfo do późniejszego użycia	444
Inne opcje wyjścia	445
Aktualizowanie innych pulpitów	447
Desktops	448
ZoomIt	450
Korzystanie z ZoomIt	450
Tryb Zoom	451
Tryb rysowania	452
Tryb wpisywania	452
Czasomierz przerwy	453
LiveZoom	454
12 Narzędzia plikowe	455
Strings	455
Streams	457
Narzędzia łączy NTFS	459
Junction	460
FindLinks	461
Disk Usage (DU)	462
Narzędzia do operacji na plikach wykonywanych po restarcie	466
PendMoves	466
MoveFile	467

13	Narzędzia dyskowe	469
	Disk2Vhd	469
	Sync	478
	DiskView	480
	Contig	484
	Defragmentowanie istniejących plików	484
	Analizowanie fragmentacji istniejących plików	486
	Analizowanie fragmentacji wolnego miejsca	487
	Tworzenie ciągłego pliku	488
	DiskExt	489
	LDMDump	490
	VolumID	492
14	Narzędzia sieciowe	495
	PsPing	495
	ICMP Ping	496
	TCP Ping	498
	Tryb serwerowy PsPing	501
	Testy opóźnień TCP/UDP	502
	Testowanie pasma TCP/UDP	504
	Histogramy PsPing	506
	TCPView	508
	Whois	510
15	Narzędzia informacji systemowej	513
	RAMMap	513
	Karta Use Counts	515
	Karta Processes	517
	Karta Priority Summary	518
	Karta Physical Pages	518
	Karta Physical Ranges	520
	Karta File Summary	520
	Karta File Details	521
	Oczyszczanie pamięci fizycznej	522
	Zapisywanie i ładowanie migawek	522
	Registry Usage (RU)	523
	CoreInfo	527
	WinObj	532

LoadOrder	535
PipeList	537
ClockRes	538
16 Różne narzędzia.....	539
RegJump.....	539
Hex2Dec	541
RegDelNull	541
Bluescreen Screen Saver.....	542
Ctrl2Cap	543

Część III: Rozwiązywanie problemów – przypadek niewyjaśniony...

17 Komunikaty błędów.....	547
Rozwiązywanie problemów z komunikatami błędów.....	548
Przypadek zablokowanego folderu	550
Przypadek pliku w użyciu	552
Przypadek „nieznanego błędu” w Przeglądarce zdjęć	554
Przypadek nieudanej rejestracji ActiveX	555
Przypadek niedziałającego Odtwarzaj do.....	558
Przypadek nieudanej instalacji	559
Rozwiązywanie problemu	560
Analiza	563
Przypadek nieczytelnych plików tekstowych	565
Przypadek brakującego skojarzenia folderu.....	567
Przypadek tymczasowych profili rejestru	570
Przypadek błędu RMS w plikach Office	576
Przypadek nieudanego podnoszenia poziomu funkcjonalnego lasu. ...	577
18 Awarie	581
Rozwiązywanie problemów z awariami.....	582
Przypadek nieudanej aktualizacji AV	585
Przypadek padającego narzędzia Proksi.....	587
Przypadek niedziałającej usługi NLA.....	588
Przypadek nieudanej aktualizacji EMET	590
Przypadek brakującego zrzutu awarii	591
Przypadek losowego spowalniania	593

19	Zawieszenia i niska wydajność	595
	Rozwiązywanie problemów z zawieszzeniami i spowolnionym działaniem	596
	Przypadek procesora zawłaszczonego przez IExplore	598
	Przypadek galopującej witryny	600
	Przypadek nadmiernego odczytywania ReadyBoost	604
	Przypadek jękającego się odtwarzacza Blue-ray	606
	Przypadek 15-minutowych logowań	610
	Przypadek zawieszających się emaili z PayPal	612
	Przypadek zawieszającego się oprogramowania księgowego	615
	Przypadek powolnej demonstracji	617
	Przypadek wolno otwierających się plików Project	623
	Złożony przypadek zawieszzeń Outlook	628
20	Złośliwe oprogramowanie	635
	Rozwiązywanie problemów ze złośliwym oprogramowaniem	636
	Stuxnet	641
	Malware i narzędzia Sysinternals	642
	Wektor infekcji wirusa Stuxnet	642
	Stuxnet w Windows XP	643
	Dalsze poszukiwania	648
	Filtrowanie w celu znalezienia interesujących zdarzeń	648
	Modyfikacje systemu wprowadzane przez Stuxnet	651
	Pliki .PNF	656
	Podniesienie uprawnień w Windows 7	659
	Stuxnet ujawniony przez narzędzia Sysinternals(?)	663
	Przypadek dziwnych restartów	663
	Przypadek fałszywej aktualizacji Java	669
	Przypadek scareware Winwebsec	672
	Przypadek galopującego GPU	683
	Przypadek niewyjaśnionych połączeń FTP	684
	Przypadek źle skonfigurowanej usługi	689
	Przypadek malware blokującego Sysinternals	693
	Przypadek malware zabijającego procesy	696
	Przypadek fałszywego komponentu systemu	698
	Przypadek tajemniczego ASEP	700

21	Zrozumieć zachowanie systemu	705
	Przypadek dysku Q:	706
	Przypadek niewyjaśnionych połączeń sieciowych	709
	Przypadek krótko żyjących procesów	711
	Przypadek rejestratora instalacji	717
	Przypadek nieznanej komunikacji NTLM	727
22	Problemy programistów	733
	Przypadek uszkodzonej delegacji Kerberos	733
	Przypadek wycieku pamięci	734
	<i>Indeks</i>	741