Microsoft

Mark Russinovich
Aaron Margosis

Windows Sysinternals

– wykrywanie i rozwiązywanie problemów

Przekład: Marek Włodarz

APN Promise, Warszawa 2017

Windows Sysinternals – wykrywanie i rozwiązywanie problemów

Authorized Polish translation of the English language edition entitled Troubleshooting with the Windows Sysinternals Tools, by Mark Russinovich and Aaron Margosis, ISBN: 978-0-7356-8444-7

Polish language edition published by APN PROMISE SA Copyright © 2017

Autoryzowany przekład z wydania w języku angielskim, zatytułowanego: Troubleshooting with the Windows Sysinternals Tools, by Mark Russinovich and Aaron Margosis, ISBN: 978-0-7356-8444-7

APN PROMISE SA, ul. Domaniewska 44a, 02-672 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

ISBN: 978-83-7541-313-7

Przekład: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Część II: Podręcznik użytkowania

Przedmowa

Nowe wydanie *Rozwiązywanie problemów przy użyciu Windows Sysinternals* jest zawsze ucztą dla umysłu i gdy mój egzemplarz dotarł do mojego wiejskiego domu w Szkocji, nastawiłem się na podróż równie fascynującą, jak mój pierwszy lot. Dziś rozumiem, że dla ludzi pozbawionych magicznych mocy (nazywam ich *Sysintuggles*) może się wydawać, że wbrew wszelkiej logice autorzy próbowali rozwiązać problem „dlaczego ludzie nie czytają instrukcji?" i jak zawsze natknęli się na krępujący wniosek „gdyż te broszurki są po prostu za małe". (I, oczywiście, przedobrzyli, tworząc tom dostatecznie duży, aby obronić się przed najbardziej drapieżnym wilkołakiem). Jednak ludzie ci po prostu nie rozumieją magii, którą ujawnia ta praca.

Zabrałem się więc do lektury. Po odpieczętowaniu okładki otworzyła się zawartość i zacząłem przewracać karty. To księga zaklęć najwyższej jakości, zaprojektowana z myślą o praktycznej magii. W połączeniu z teorią zawartą w *Windows Internals* zapewni Czytelnikowi najlepsze wykształcenie, jakiego może poszukiwać dzisiejszy mag. Przy użyciu przedstawionych tu eliksirów i zaklęć możliwe staje się dokonywanie prawdziwie znaczących rzeczy. Nauczy Czytelnika, jak czarować Windows i zaklinać malware. Pokaże, jak zamknąć dżiny w butelkach, warzyć rozwiązania, a nawet zakorkować bluescreeny. Zacząłem opatrywać moją księgę uwagami, pozaginałem rogi kart i pisałem powiązane zaklęcia na marginesach, a wkrótce uzyskałem niezastąpioną pomoc. Zajmuje honorowe miejsce na mojej podręcznej półce.

Jest to potężna pomoc dla prawdziwie zaawansowanej magii. Jeśli jesteś odpowiedzialny za administrowanie systemami gdziekolwiek, małymi lub wielkimi, na pewno znajdzie się coś, czego nauczysz się z tej książki. Profesor Russinovich zaprawdę jest najbystrzejszym czarodziejem naszych czasów; on i jego elfy stworzyli niezastąpione dzieło.

Noted Person

Maj 2016

Wstęp

Sysinternals Suite to zbiór przeszło 70 zaawansowanych narzędzi diagnostycznych i naprawczych dla platformy Microsoft Windows, napisanych przeze mnie – Marka Russinovicha – oraz Bryce'a Cogswella. Od czasu przejęcia firmy Sysinternals przez Microsoft w roku 2006 narzędzia te zostały udostępnione do pobrania bez opłat z utrzymywanej przez Microsoft witryny Windows Sysinternals (stanowiącej część Microsoft TechNet).

Celem tej książki jest zapoznanie Czytelnika z narzędziami Sysinternals oraz ułatwienie ich pełnego wykorzystania. Książka zawiera również rzeczywiste, z życia wzięte przykłady pokazujące, jak ja sam i inni użytkownicy Sysinternals wykorzystują te narzędzia do rozwiązywania problemów spotykanych w systemach Windows.

Choć napisałem tę książkę wspólnie z Aaronem Margosisem, cały tekst został sformułowany tak, jakbym to ja sam mówił. Nie jest to żaden przytyk do udziału Aarona w powstaniu tej książki; bez jego ciężkiej pracy ten tom w ogóle by nie istniał.

Uwaga Podrozdział „Ostatnie zmiany" w dalszej części Wstępu zawiera informacje o aktualizacjach i uzupełnieniach, które nastąpiły w trakcie przygotowań do wydania książki.

Omawiane narzędzia

Książka ta zawiera omówienie wszystkich narzędzi z zestawu Sysinternals, które są dostępne w witrynie Windows Sysinternals (*http://technet.microsoft.com/en-us/sysinternals/default.aspx*) i wszystkich ich funkcji zgodnie ze stanem w chwili pisania tych słów (początek lata 2016 roku). Jednak Sysinternals jest tworem wysoce dynamicznym: istniejące narzędzia regularnie uzyskują nowe możliwości, a od czasu do czasu wprowadzane są nowe programy. (Chcąc być na bieżąco, można śledzić strumień RSS bloga „Sysinternals Site Discussion" pod adresem *http://blogs.technet.microsoft.com/sysinternals/*). Możliwe jest zatem, że w chwili czytania tej książki niektóre fragmenty mogą być zdezaktualizowane. Tym niemniej należy zawsze dbać o to, aby narzędzia Sysinternals były aktualizowane do najnowszej wersji, aby móc wykorzystać nowe funkcjonalności i poprawki.

Książka nie obejmuje narzędzi, które zostały uznane za przestarzałe i nie są już dostępne w witrynie Sysinternals. Jeśli ktoś nadal używa takich narzędzi, jak Regmon

(Registry Monitor) lub Filemon (File Monitor), powinien zastąpić je narzędziem Process Monitor, opisanym w rozdziale 5. Z kolei Rootkit Revealer, jeden z pierwszych w branży detektorów rootkitów (to właśnie to narzędzie wykryło osławiony „Sony rootkit") dobrze spełnił swoją rolę i został już wycofany. Analogicznie kilka innych narzędzi (takich jak Newsid i EfsDump), które zapewniały unikatowe możliwości, zostało wycofanych, gdyż albo nie są już potrzebne, albo równoważna funkcjonalność została wreszcie dodana do samego systemu Windows.

Historia Sysinternals

Pierwszy program Sysinternals, który napisałem, Ctrl2cap, narodził się z konieczności. Zanim zacząłem używać Windows NT w roku 1995, posługiwałem się głównie systemami UNIX, które miały klawiatury z klawiszem Ctrl umieszczonym w tym miejscu, w którym na standardowej klawiaturze PC znajduje się Caps Lock. Zamiast dostosowywać się do nowego (dla mnie) układu, zdecydowałem się poznać zasady tworzenia sterowników urządzeń Windows NT i napisałem sterownik, który zamieniał naciśnięcia klawisza Caps Lock na wciśnięcia klawisza Ctrl w trakcie przekazywania impulsu od klawiatury do systemu wejścia Windows NT. Ctrl2cap nadal jest obecny w witrynie Sysinternals i używam go na wszystkich swoich komputerach.

Ctrl2cap był pierwszym z wielu narzędzi, które napisałem, aby lepiej poznać to, jak działają Windows NT, jednocześnie zapewniając pewne przydatne funkcjonalności. Kolejne napisane narzędzie, NTFSDOS, zaprojektowałem wspólnie z Bryce'm Cogswellem. Poznaliśmy się na studiach podyplomowych w Carnegie Mellon University, gdzie wspólnie napisaliśmy kilka artykułów naukowych i pracowaliśmy w nowo powstałej firmie, w której projektowaliśmy oprogramowanie dla systemu Windows 3.1. Wpadłem na pomysł narzędzia, które pozwoliłoby użytkownikom odczytywać dane z partycji sformatowanej jako NTFS przy użyciu wszechobecnych dyskietek DOS. Bryce uznał to za zabawne wyzwanie programistyczne; podzieliśmy pracę pomiędzy siebie i pierwszą działającą wersję opublikowaliśmy około miesiąca później.

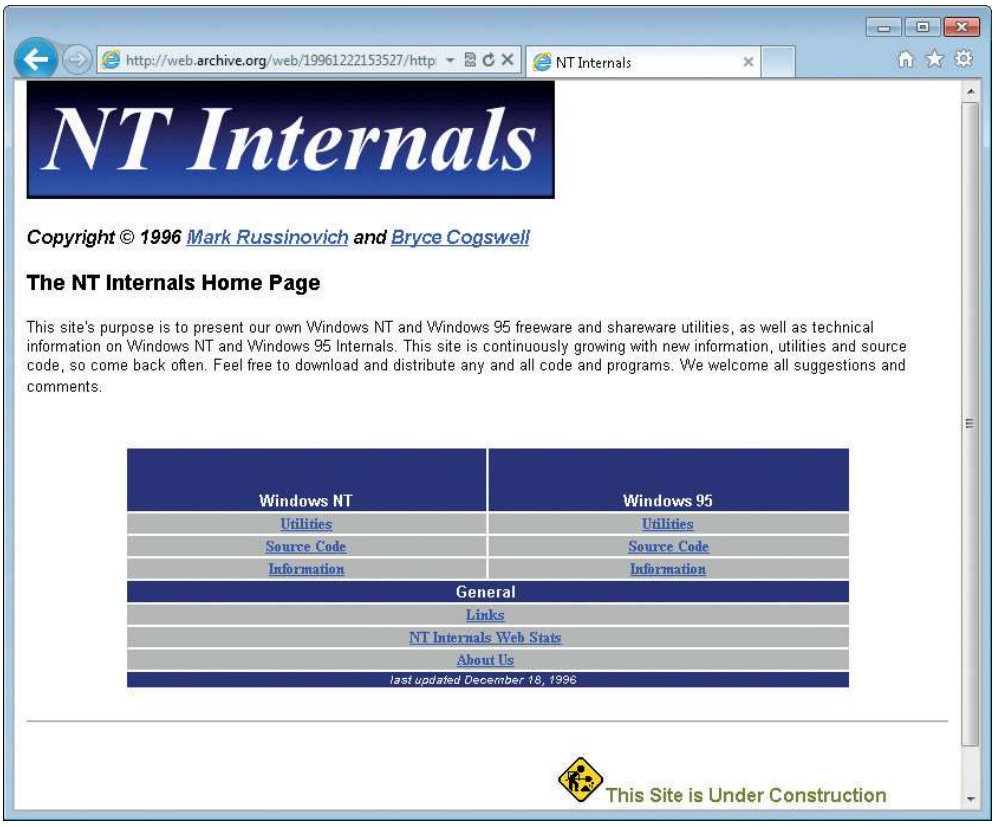
Wspólnie z Bryce'm napisałem również dwa kolejne narzędzia, Filemon i Regmon. Te trzy programy – NTFSDOS, Filemon i Regmon – stały się fundamentem Sysinternals.

Filemon i Regmon, które obydwa powstały w wersjach dla systemu Windows 95 i dla Windows NT, pokazywały na bieżąco aktywność systemu plików i rejestru, będąc pierwszymi narzędziami, które go umożliwiały, a tym samym stały się niezbędną pomocą w rozwiązywaniu problemów.

Bryce i ja zdecydowaliśmy się udostępnić te narzędzia innym, ale nie mieliśmy wówczas własnej witryny, zatem początkowo publikowaliśmy je na stronie naszego przyjaciela, Andrew Schulmana, którego poznałem w związku z jego własną pracą odkrywania wewnętrznych operacji w systemach DOS i Windows 95. Korzystanie

z pośrednika nie pozwalało jednak na aktualizowanie i poprawianie bugów tak szybko, jak chcieliśmy, zatem we wrześniu 1996 utworzyliśmy witrynę NTInternals.com, hostującą zarówno narzędzia, jak i artykuły na temat wewnętrznego działania Windows 95 i Windows NT. Bryce i ja zaprojektowaliśmy również narzędzia, które zamierzaliśmy sprzedawać w celu osiągnięcia jakiegoś dodatkowego dochodu, zatem w tym samym miesiącu założyliśmy Winternals Software, komercyjną firmę programistyczną, którą promowaliśmy poprzez prosty baner reklamowy na stronie NTInternals.com. Pierwszym narzędziem opublikowanym pod szyldem Winternals Software było NTRecover, narzędzie pozwalające zamontować dyski z niedającego się uruchomić systemu Windows NT w działającym systemie i uzyskiwać do nich dostęp, jakby były to dyski podłączone lokalnie.

Misja witryny NTInternals.com polegała na upowszechnianiu narzędzi *freeware*, które wykorzystywały naszą coraz szerszą wiedzę o systemach operacyjnych Windows w celu udostępniania wydajnych możliwości diagnostyki, monitorowania i zarządzania. W ciągu kilku miesięcy witryna, której wygląd w grudniu 1996 pokazuje poniższy zrzut ekranu (dostępny dzięki Internet Archive Wayback Machine) przyciągnęła 1500 odwiedzin dziennie, co czyniło ją jedną z najbardziej popularnych witryn narzędziowych dla systemu Windows w tych wczesnych dniach rewolucji internetowej. W roku 1998, „zachęceni" przez prawników firmy Microsoft, zmieniliśmy nazwę witryny na Sysinternals.com.



W ciągu kolejnych kilku lat narzędzia stale ewoluowały. Dodawaliśmy kolejne programy w miarę tego, jak potrzebowaliśmy ich sami, ale również pod wpływem sugestii ulepszeńpochodzących od pierwszych użytkowników, a także wtedy, gdy wymyśliliśmy jakiś nowy sposób pokazania informacji o działaniu Windows.

Narzędzia Sysinternals podzieliły się na trzy podstawowe kategorie: mające pomagać programistom, służące do rozwiązywania problemów oraz te, które wspomagały zarządzanie systemami. DebugView, program przechwytujący i wyświetlający wyrażenia debugowania, był jednym z wczesnych narzędzi programistycznych, które napisałem na własny użytek jako pomoc w tworzeniu sterowników urządzeń. DLLView, narzędzie pokazujące biblioteki DLL ładowane przez procesy, oraz HandleEx, graficzne narzędzie prezentujące procesy, które ukazywało otwarte dojścia, były pierwszymi dwoma narzędziami nastawionymi na rozwiązywanie problemów. (W roku 2001 połączyłem funkcjonalność DLLView i HandleEx, aby utworzyć Process Explorer). Zestaw PsTools, omówiony w rozdziale 7, zawiera kilka najbardziej popularnych narzędzi zarządzania, zebranych w pakiet dla ułatwienia pobierania. PsList, pierwsze narzędzie z tej grupy, powstał z inspiracji poleceniem ps systemów uniksowych, które zwraca listę działających procesów. Narzędzia rozrastały się zarówno pod względem liczby, jak i funkcjonalności, stając się zestawem oprogramowania narzędziowego pozwalającego na łatwe wykonywanie wielu zadańw systemach zdalnych bez konieczności wcześniejszego instalowania w tych systemach jakiegoś specjalnego oprogramowania.

Również w 1996 roku zacząłem pisać artykuły dla magazynu Windows IT Pro, poświęcone wewnętrznym mechanizmom Windows i narzędziom Sysinternals, a także rozmaite dodatkowe teksty, w tym dość kontrowersyjny artykuł z 1996 roku, przez który moje nazwisko stało się znane w samej firmie Microsoft, choć niekoniecznie w pozytywny sposób. Artykuł ten, „Inside the Difference Between Windows NT Workstation and Windows NT Server", wskazywał na bardzo ograniczone różnice pomiędzy Windows NT Workstation a Windows NT Server, co było sprzeczne z komunikatem marketingowym firmy Microsoft.

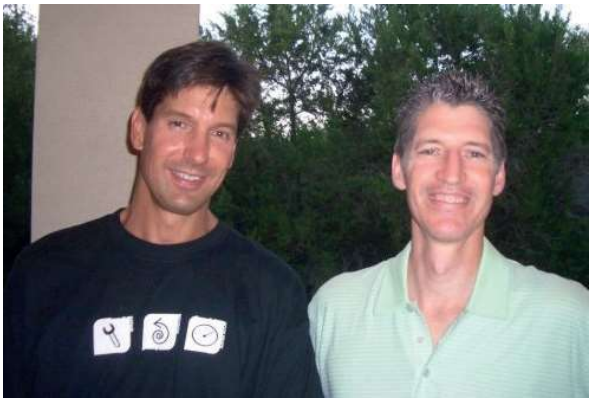
Negatywny pogląd firmy Microsoft na mój temat pogorszyło jeszcze opublikowanie Ntcrash i Ntcrash2, narzędzi nazywanych dziś „fuzzers", które ostrzeliwały interfejs wywołań systemowych Windows NT losowymi śmieciami. Narzędzia te zidentyfikowały kilkadziesiąt wywołańsystemowych, które miały słabą weryfikację parametrów wejściowych, prowadzących do uszkodzenia zawartości pamięci i – ostatecznie – do *blue-screen*, pomimo działania jako procesy nieuprzywilejowanego trybu użytkownika. (W latach dziewięćdziesiątych takie zjawiska były postrzegane jako bugi niezawodności i co najwyżej kłopotliwe – dziś sklasyfikowano by je jako „poważne" błędy zabezpieczeń).

W miarę jak narzędzia rozwijały się i ewoluowały, zacząłem rozważać napisanie książki na temat wewnętrznych mechanizmów Windows. Ta książka już w istocie istniała, *Inside Windows NT* (Microsoft Press, 1992), której pierwsze wydanie zostało napisane przez Helen Custer jednocześnie z oryginalną wersją Windows NT 3.1.

Drugie wydanie zostało przeredagowane i uzupełnione pod kątem Windows NT 4.0 przez Davida Solomona, dobrze znanego eksperta, wykładowcę i autora, który pracował w firmie DEC. Zamiast pisania książki od początku, skontaktowałem się z nim i zaproponowałem współpracę nad trzecim wydaniem, które miało objąć wersję Windows 2000. Moje kontakty z firmą Microsoft poprawiły się nieco od czasu artykułu z 1996 roku dzięki wysyłaniu zgłoszeń wykrytych przeze mnie bugów bezpośrednio do projektantów systemu Windows, ale David nadal musiał uzyskać zgodę Microsoftu na moje współautorstwo, którą ostatecznie otrzymał.

W rezultacie David Solomon i ja wspólnie napisaliśmy trzecie, czwarte, piąte i szóste wydanie książki, której tytuł zmieniono na *Windows Internals* w wydaniu czwartym. W wydaniu piątym zaprosiliśmy Alexa jako współautora. W szóstym wydaniu zawartość rozrosła się tak bardzo, że musieliśmy podzielić książkę na dwie części. Niedługo po tym, jak ukończyliśmy *Inside Windows 2000* (Microsoft Press, 2000), dołączyłem do Davida jako wykładowca na jego seminariach o wewnętrznych mechanizmach Windows, dodając swoją własną treść. Oferowane na całym świecie, nawet w firmie Microsoft, gdzie słuchaczami byli projektanci Windows, wykłady te intensywnie wykorzystywały narzędzia Sysinternals, aby pokazać studentom, jak można zajrzeć do wnętrza Windows i nauczyć się więcej o rzeczach, które przydały się im później, gdy wracali do swoich ról programistów i profesjonalistów IT.

W roku 2006 moje kontakty z firmą Microsoft były już silne i dobre od wielu lat. Firma Winternals dysponowała kompletnym zbiorem oprogramowania zarządzającego i rozrosła się do około 100 pracowników, zaś witryna Sysinternals miała ponad dwa miliony pobrań miesięcznie. 18 lipca 2006 Microsoft zakupił zarówno Winternals, jak i Sysinternals. Niedługo później Bryce i ja (to my w roku 2006 na zdjęciu poniżej) przenieśliśmy się do Redmond, aby stać się częścią zespołu Windows. Obecnie pełnię funkcję Chief Technology Officer of Microsoft Azure, kierując strategiami technicznymi i architekturą platformy chmurowej Azure.



Nabycie Sysinternals (i Winternals) przez Microsoft miało dwa cele: zapewnienie, że narzędzia zaprojektowane przez Bryce'a i mnie będą nadal dostępne za darmo i że społeczność, którą zbudowaliśmy, będzie kwitnąć – i zostały one osiągnięte. Dziś

Windows Sysinternals w ramach *technet.microsoft.com* jest jedną z najczęściej odwiedzanych witryn TechNet, osiągając około 4,5 miliona pobrań miesięcznie. Zaawansowani użytkownicy Sysinternals wracają wielokrotnie po najnowsze wersje narzędzi, a także po nowe, takie jak niedawno opublikowane Sysmon i PsPing, a także w celu uczestniczenia w społeczności Sysinternals, stale rosnącego forum z przeszło 42 tysiącami zarejestrowanych użytkowników w chwili pisania tych słów. Ja zaś nadal kontynuuję ulepszanie istniejących narzędzi i dodawanie nowych.

Wiele osób sugerowało już dawno, że książka na temat tych narzędzi byłaby wartościowa, ale to David Solomon powiedział, że jest to bardzo spóźniony projekt, gdy wreszcie się za to zabrałem. Moje obowiązki w firmie Microsoft nie pozwalały mi na poświęcenie czasu niezbędnego na napisanie kolejnej książki, ale David zauważył, że mógłbym znaleźć kogoś do pomocy. Byłem uszczęśliwiony, że Aaron Margosis zgodził się na współpracę ze mną. Aaron pełni funkcję głównego konsultanta Microsoft Cybersecurity Services i jest dobrze znany ze swojej wiedzy na temat zagadnień bezpieczeństwa systemu Windows i kompatybilności aplikacji. Znam Aarona od wielu lat i jego doskonałe umiejętności pisarskie, znajomość wewnętrznych mechanizmów Windows i sprawność w posługiwaniu się narzędziami Sysinternals czynią go idealnym współautorem.

Kto powinien przeczytać tę książkę

Książka ta przeznaczona jest dla profesjonalistów IT, zaawansowanych użytkowników, a także programistów, którzy chcą wydobyć jak najwięcej z narzędzi Sysinternals. Bez względu na doświadczenie w korzystaniu z tych narzędzi, a także bez względu na to, czy Czytelnik zarządza systemami w wielkim przedsiębiorstwie, w małym biznesie, czy też komputerami swojej rodziny i przyjaciół, na pewno znajdzie tu nowe narzędzia, zdobędzie wskazówki i pozna techniki pomagające w bardziej skutecznym rozwiązywaniu najtrudniejszych problemów i upraszczające codzienne operacje zarządzania systemami i monitorowania.

Założenia

Oczekuje się, że Czytelnik dobrze zna system operacyjny Windows. Podstawowa znajomość takich koncepcji, jak procesy, wątki, pamięć wirtualna oraz tryb wiersza poleceń Windows będzie pomocna, choć niektóre z tych zagadnień zostaną omówione w rozdziale 2, „Kluczowe koncepcje systemu Windows".

Organizacja książki

Książka podzielona jest na trzy części. Część I, „Zaczynamy", zapewnia przegląd narzędzi i witryny Sysinternals, opisuje funkcjonalności wspólne dla wszystkich narzędzi, wyjaśnia, gdzie udać się w poszukiwaniu pomocy, a także omawia niektóre podstawowe koncepcje systemu Windows, co pozwoli lepiej poznać samą platformę i zrozumieć informacje zwracane przez poszczególne narzędzia.

Część II, „Podręcznik użytkowania", jest szczegółowym przewodnikiem po wszystkich funkcjach narzędzi Sysinternals, opcjach wiersza poleceń, wymaganiach systemowych i pułapkach. Dzięki licznym zrzutom ekranowym i przykładom część ta powinna zapewnić odpowiedź na niemal każde pytanie, jakie można postawić. Głównym narzędziom, takim jak Process Explorer i Process Monitor, poświęcono oddzielny rozdział; pozostałe rozdziały omawiają narzędzia według kategorii zastosowań, takich jak narzędzia dotyczące zabezpieczeń, Active Directory czy systemu plików.

Część III, „Rozwiązywanie problemów – Przypadek niewyjaśniony…", zawiera historie rozwiązywania rzeczywistych problemów przy użyciu narzędzi Sysinternals, pochodzące z doświadczeń Aarona i moich, a także nadesłane przez administratorów i innych użytkowników z całego świata.

Konwencje używane w książce

Książka ta prezentuje informacje przy użyciu pewnych konwencji mających na celu zwiększenie czytelności i łatwości śledzenia informacji:

- Elementy w ramkach z nagłówkami takimi jak „Uwaga" zapewniają dodatkowe informacje lub alternatywne metody wykonania zadania.
- Tekst wpisywany przez Czytelnika (poza blokami kodu) został wyróżniony **wytłuszczeniem**.
- Znak plus (+) pomiędzy nazwami dwóch klawiszy oznacza, że klawisze te muszą zostać naciśnięte jednocześnie. Na przykład „Naciśnij Alt+Tab" oznacza, że należy przytrzymać klawisz Alt, gdy naciskamy Tab.
- Pionowa kreska pomiędzy nazwami elementów menu (na przykład File | Close) oznacza, że należy wybrać pierwszy element, a następnie kolejny z menu podrzędnego[1].
- W specyfikacji składni wiersza polecenia pionowa kreska oznacza „albo", nawiasy kwadratowe oznaczają elementy opcjonalne, tekst pisany kursywą jest symbolem

1 W przypadku elementów systemowych, które dostępne są w wersji zlokalizowanej (np. polskiej), przy pierwszym użyciu elementu menu podana zostanie polska wersja danej pozycji (w nawiasie). Narzędzia Sysinternals są dostępne tylko w wersji angielskiej. (przyp. tłum.).

zastępczym, który należy zastąpić informacjami właściwymi dla środowiska użytkownika, nawiasy klamrowe oznaczają grupowanie, zaś wielokropki – powtarzający się wzorzec. Rozważmy poniższy przykład:

```
procdump
    [-ma | -mp | -d callback_DLL] [-64] [-r [1..5] [-a]] [-o]
    [-n count] [-s secs]
    [-c|-cl percent [-u]] [-m|-ml commit] [-p|-pl counter_threshold]
    [-e [1 [-g] [-b]]] [-h] [-l] [-t] [-f filter,...]
    {
      {{[-w] process_name}|service_name|PID }
        [dump_file | dump_folder] } |
        {-x dump_folder image_file [arguments]}
    }
```

Zapis ten oznacza, że można opcjonalnie użyć przełączników **–ma**, **–mp** lub **–d**; jeśli użyjemy **–d**, trzeba dostarczyć wartość dla *callback_DLL*. Można również zdecydować się na użycie opcji **–f**; w takim przypadku konieczne jest dostarczenie jednej lub więcej wartości *filter*. Grupowanie w ostatnich czterech wierszach pokazuje, że konieczne jest wyspecyfikowanie elementów *process_name*, *service_name* albo *PID*, lub użycie opcji **–x** ze wskazaniem parametrów *dump_folder* i *image_file*.

Wymagania systemowe

Narzędzia Sysinternals działają w następujących wersjach systemu operacyjnego Windows, włącznie z wydaniami 64-bitowymi, o ile nie zostanie inaczej zaznaczone:

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10 (desktop)[2]
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016, w tym Nano Server

Niektóre narzędzia wymagają do działania uprawnień administracyjnych. Inne mogą zawierać funkcjonalności, które wymagają uprawnieńadministracyjnych.

2 Wszystkie narzędzia Sysinternals to aplikacje Win32, wspierające tylko architektury x86 oraz x64; nie są one kompatybilne z wersjami Windows 10 Mobile, IoT, Xbox itp.

Ostatnie zmiany

W chwili, gdy kończyliśmy pracę nad tą książką, opublikowałem zaktualizowane wersje wielu narzędzi w celu obsługi wydania Nano Server systemu Windows Server 2016. Nano Server to zminimalizowana, pozbawiona interfejsu użytkownika opcja instalacyjna Windows Server 2016, zawierająca tylko podstawowy zestaw funkcji i usług. Z punktu widzenia użytkowników Sysinternals istotny jest fakt, że Nano Server nie zawiera podsystemu 32-bitowego ani komponentów GUI. Jak opisałem w rozdziale 1, „Początki pracy z narzędziami Sysinternals", każdy program Sysinternals jest zawsze spakowany jako pojedynczy 32-bitowy plik wykonywalny, przy czym wszystkie dodatkowe wymagane pliki, takie jak binaria 64-bitowe, są osadzone jako zasoby, które mogą zostać wydobyte i uruchomione w razie potrzeby. Oczywiście żaden z tych 32-bitowych obrazów nie będzie działał w Nano Server, zatem utworzyłem natywne 64-bitowe wersje narzędzi trybu konsolowego, dodając człon „64.exe" do ich nazw plików. Na przykład 64-bitowa wersja SigCheck.exe to SigCheck64.exe. Dodatkowo utworzyłem wersję trybu konsolowego narzędzia LoadOrd (Load Order) o nazwie LoadOrdC.exe, a także natywną wersję 64-bitową, LoadOrdC64.exe.

Zarządzanie Nano Server polega głównie na mechanizmie PowerShell Remoting. Powłoka PowerShell traktuje dowolne wyjście do standardowego strumienia błędu (*stderr*) jako sygnalizację błędu. Narzędzia trybu konsoli Sysinternals zawsze zapisywały swoje informacje baneru i składni do *stderr*. Aby usprawnić obsługę narzędzi w powłoce PowerShell, a w szczególności w Nano Server, narzędzia te obecnie zapisują informacje baneru i składni do strumienia standardowego wyjścia (*stdout*) i używają nowej opcji wiersza polecenia **–nobanner**, powodującą pominięcie baneru. Warto zauważyć, że zastępuje to opcję **–q**, której wiele narzędzi używało do tego samego celu.

Podziękowania

Przede wszystkim Aaron i ja chcielibyśmy podziękować Bryce'owi Cogswellowi, współtwórcy Sysinternals, za jego nieoceniony wkład w powstawanie narzędzi Sysinternals. Dzięki naszej współpracy to, co Bryce i ja opublikowaliśmy w Sysinternals, było czymś dużo większym, niż prosta suma indywidualnych wysiłków. Bryce odszedł z Microsoft w październiku 2010 roku i życzymy mu powodzenia we wszystkim, co podejmie.

Chcemy też podziękować Davidowi Solomonowi za przymuszenie Marka do napisania tej książki, a także szczegółowe przejrzenie wielu rozdziałów i napisanie przedmowy do pierwszego wydania. Dave jest też jednym z najbardziej skutecznych propagatorów Sysinternals od wielu lat i to z jego inspiracji powstało wiele wartościowych funkcjonalności.

Podziękowania należą się też Luke'owi Kim za nieocenioną pomoc w aktualizowaniu projektów do najnowszych wersji Microsoft Visual Studio, przeniesieniu narzędzi

systemu kontroli źródeł Visual Studio Team Services (VSTS), uporządkowaniu procesu kompilacji i publikowania i zarządzaniu witryną Sysinternals.com i serwerami infrastruktury live.sysinternals.com (działających w chmurze Azure). Dziękujemy też Kentowi Sharkey za publikowanie aktualizacji w Sysinternals.com.

Jeszcze kilka lat temu Bryce i ja byliśmy jedynymi autorami narzędzi, ale od pewnego czasu zacząłem akceptować wkład innych programistów. Ken Johnson, Andrew Richards, Thomas Garnier, David Magnotti, Dmitry Davydok, Daniel Pearson, Justin Jiang i cała reszta zespołu Nano Server, Giulia Biagini, Pavel Yosifovich i Aaron Margosis – wszyscy oni dodali znaczące funkcjonalności do poszczególnych narzędzi.

Wielkie dzięki kierujemy do Johna Sheehana za pomoc w opisaniu wcześniej nieudokumentowanych szczegółów działania AppContainers; do Alexa Ionescu za materiał dotyczący chronionych procesów; a także do Neda Pyle'a, Marty Lichtela i Carla Harrisona za zgodę na włączenie do książki przypadków, które wcześniej opublikowali.

Jesteśmy wdzięczni następującym osobom, którzy wykonali żmudną pracę redakcji technicznej, korekty i poprawek w tym wydaniu książki: Andrew Richards, Bhaskar Rastogi, Bruno Aleixo, Burt Harris, Chris Jackson, Crispin Cowan, Greg Cottingham, Ken Johnson (*aka* Skywing), Luke Kim, Mario Raccagni, Steve Thomas i Yong Rhee.

Początkowo wydawało nam się, że zwrócenie się do *Noted Person* o napisanie przedmowy do tego wydania jest zbytnią zuchwałością, i nadal fascynuje nas to, że się zgodził. Dziękujemy, N.P.[3]

Aaron chciałby podziękować swojej żonie Elise i dzieciom –Elanie, Jonahowi i Gabrielowi – za ich miłość i wsparcie. Ponadto chcę podziękować Brendzie Schrier za fotografię na stronie autorskiej. Na koniec Aaron chce podziękować Washington Nationals Baseball Club oraz West Ham United F.C.

Mark dziękuje swojej żonie Daryl i córce Marii za wspieranie wszystkich jego przedsięwzięć.

Errata, aktualizacje i pomoc dotycząca książki

Dołożyliśmy wszelkich starań, aby zapewnić dokładność i precyzję informacji zawartych w książce. Listę dostrzeżonych błędów będziemy w razie potrzeby publikować na stronie *http://aka.ms/TroubleshootSysint/errata*

W przypadku natrafienia na błąd, który nie został tam jeszcze uwzględniony i skorygowany, można zgłosić go poprzez tę samą stronę.

Jeśli potrzebna jest dodatkowa pomoc, prosimy o e-mail do Microsoft Press Book Support pod adresem *mspinput@microsoft.com*.

3 ***Noted Person*** to tajna tożsamość ***Chrisa Jacksona***, podpisującego się również jako ***The App Compat Guy*** oraz ***Captain Inappropriate***.

Proszę zauważyć, że pod tymi adresami nie jest oferowana pomoc techniczna dotycząca produktów firmy Microsoft. W sprawie pomocy dotyczącej oprogramowania lub sprzętu firmy Microsoft proszę skierować się do *http://support.microsoft.com*.

Bezpłatne ebooki z Microsoft Press

Poczynając od przeglądów technicznych, aż po pogłębione informacje na szczegółowe tematy, bezpłatne ebooki z Microsoft Press obejmują wielki zakres tematyki. Ebooki te dostępne są w formatach PDF, EPUB i Mobi for Kindle, gotowe do pobrania ze strony:

http://aka.ms/mspressfree

Warto często sprawdzać, co nowego!

Pozostańmy w kontakcie

W wydawnictwie Microsoft Press satysfakcja czytelników jest najwyższym priorytetem, a uzyskiwane informacje zwrotne są najcenniejszym zasobem. Napiszcie nam, co myślicie o tej książce:

http://aka.ms/tellpress

Ankieta jest krótka, a my czytamy każdy komentarz. Dziękujemy z góry!

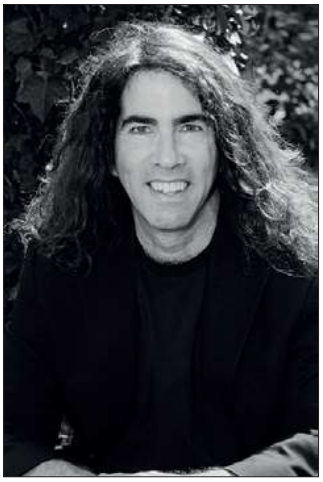
Jesteśmy też na Twitterze:

http://twitter.com/MicrosoftPress.

O autorach

Mark Russinovich zajmuje stanowisko Chief Technology Officer w Microsoft Azure, gdzie nadzoruje strategie techniczne i architekturę platformy chmurowej firmy Microsoft. Jest szeroko znanym ekspertem od systemów rozproszonych, wewnętrznych mechanizmów systemów operacyjnych i cyberbezpieczeństwa. Jest autorem powieści z gatunku cyberthrillerów: *Zero Day*, *Trojan Horse* i *Rogue Code*, ze wspólnym bohaterem Jeffem Aikenem, będącym *alter ego* autora, a także współautorem wydanych przez Microsoft Press książek *Windows Internals*. Russinovich dołączył do Microsoft w 2006 roku, gdy Microsoft zakupił Winternals Software, firmę założoną przez niego w roku 1996, a także witrynę Sysinternals, w której publikuje i omawia dziesiątki popularnych narzędzi diagnostycznych i administracyjnych. Często występuje na najważniejszych konferencjach branżowych, w tym Microsoft Ignite, Microsoft //build, RSA Conference i wielu innych.

Można się z nim skontaktować pod adresem *markruss@microsoft.com* lub na Twitterze pod *https://www.twitter.com/markrussinovich*.



Aaron Margosis pełni funkcję Principal Consultant w Global Cybersecurity Practice należącej do firmy Microsoft, gdzie pracuje od roku 1999. Aaron specjalizuje się w zagadnieniach bezpieczeństwa systemu Windows, minimalizowania potrzebnych przywilejów, kompatybilności aplikacji i konfigurowana zamkniętych środowisk. Występuje na wielu konferencjach, a także stworzył wiele narzędzi używanych w organizacjach implementujących środowiska wysokiego poziomu zabezpieczeń, w tym LUA Buglight, Policy Analyzer, IE Zone Analyzer, LGPO.exe (narzędzie do przetwarzania lokalnego obiektu zasad grupy) oraz MakeMeAdmin, które można pobrać z jego blogu (*https://blogs.msdn.microsoft.com/aaron_margosis*) lub z blogów dwóch zespołów, w których jest podstawowym autorem (*https://blogs.technet.microsoft.com/fdcc* oraz *https://blogs.technet.microsoft.com/SecGuide*).

Można się z nim skontaktować pod adresem *aaronmar@microsoft.com* lub na Twitterze pod *https://www.twitter.com/AaronMargosis*.

CZĘŚĆ I

Zaczynamy

ROZDZIAŁ 1

Wprowadzenie do narzędzi Sysinternals

Mianem *Sysinternals* określamy zestaw bezpłatnych, zaawansowanych narzędzi administracyjnych, diagnostycznych i naprawczych dla platformy systemowej Microsoft Windows, napisanych przez założycieli Sysinternals: mnie (Marka Russinovicha) i Bryce'a Cogswella. Od czasu przejęcia Sysinternals przez firmę Microsoft w lipcu 2006 roku narzędzia te są dostępne w witrynie Microsoft TechNet.

Cechy charakterystyczne narzędzi Sysinternals to:

- Zaspokajają potrzeby profesjonalistów IT i programistów, których nie rozwiązują inne środki.
- Są intuicyjne i łatwe w użyciu.
- Są spakowane jako pojedynczy obraz wykonywalny (.exe), który nie wymaga instalacji i może zostać uruchomiony z dowolnego miejsca, w tym z lokalizacji sieciowych lub nośników wymiennych.
- Nie pozostawia w systemie żadnych znaczących, przypadkowych danych po uruchomieniu.

Ponieważ Sysinternals nie mają nadmiarowości formalnej grupy produktowej, mogę szybko publikować nowe funkcje, narzędzia i poprawki. W niektórych przypadkach mogę przekształcić sugestie użytkowników w użyteczną, a łatwą do wdrożenia funkcjonalność w czasie nieprzekraczającym tygodnia.

Tym niemniej istnieje również druga strona nie posiadania pełnej grupy produktowej i formalnej organizacji testowej – narzędzia są udostępniane „tak jak są", bez oficjalnego wsparcia produktowego firmy Microsoft. Zespół Sysinternals utrzymuje dedykowane forum wsparcia społecznościowego – opisane dalej w tym rozdziale – w witrynie Sysinternals, i staram się naprawiać zgłaszane błędy i bugi tak szybko, jak to możliwe.

Przegląd narzędzi

Narzędzia Sysinternals obejmują szeroki zakres funkcjonalności dotyczący licznych aspektów systemu operacyjnego Windows. Podczas gdy niektóre z bardziej wyrafinowanych narzędzi, takie jak Process Explorer i Process Monitor, rozciągają się na wiele kategorii operacji, inne można lepiej lub gorzej pogrupować w określone kategorie, takie jak „narzędzia procesów" lub „narzędzia plików". Wiele z nich dysponuje graficznym interfejsem użytkownika (GUI), podczas gdy inne są narzędziami konsolowymi, wyposażonymi w liczne przełączniki zaprojektowane z myślą o automatyzacji lub uruchamianie w trybie wiersza poleceń.

Książka ta zawiera omówienie czterech głównych narzędzi (Process Explorer, Autoruns, Process Monitor oraz ProcDump), przy czym każdemu poświęciłem oddzielny rozdział. W dalszych rozdziałach opisuję po wiele narzędzi, pogrupowanych według kategorii.

Tabela 1-1 zawiera listę tych rozdziałów z krótkim przedstawieniem każdego z narzędzi w nich omawianych.

Tabela 1-1 Tematyka rozdziałów

Narzędzie	Opis
Rozdział 3, Process Explorer	
Process Explorer	Zastępuje Task Manager (Menedżer zadań) i wyświetla znacznie bardziej szczegółowe dane o procesach i wątkach, w tym zależność nadrzędny/podrzędny, załadowane biblioteki DLL oraz otwarte dojścia do obiektów, takie jak pliki w użyciu.
Rozdział 4, Autoruns	
Autoruns	Wylicza i klasyfikuje oprogramowanie skonfigurowane do automatycznego uruchamiania podczas rozruchu systemu, logowania użytkownika lub przy uruchamianiu Internet Explorer, jednocześnie pozwalając na wyłączenie lub usunięcie tych wpisów.
Rozdział 5, Process Monitor	
Process Monitor	Rejestruje szczegóły o całej aktywności dotyczącej systemu plików, rejestru, sieci, procesów, wątków i ładowania obrazów w czasie rzeczywistym.
Rozdział 6, ProcDump	
ProcDump	Generuje zrzut pamięci dla procesu, gdy ten spełni określone kryteria, takie jak wywołanie szczytu obciążenia CPU lub nieodpowiadające okno.

Tabela 1-1 Tematyka rozdziałów

Narzędzie	Opis
Rozdział 7, PsTools	
PsExec	Zdalnie uruchamia procesy, jako Local System, z przekierowaniem wyjścia, lub obydwa.
PsFile	Wylicza i pozwala zamknąć pliki otwarte zdalnie.
PsGetSid	Wyświetla identyfikator zabezpieczeń (Security Identifier – SID) podmiotu zabezpieczeń, takiego jak komputer, użytkownik, grupa lub usługa.
PsInfo	Wylicza informacje o systemie.
PsKill	Kończy procesy wskazane poprzez nazwę lub identyfikator (PID).
PsList	Wyświetla szczegółowe informacje o procesach i wątkach.
PsLoggedOn	Wylicza konta, które są zalogowane lokalnie lub za pośrednictwem połączeńzdalnych.
PsLogList	Zrzuca rekordy dziennika zdarzeń.
PsPasswd	Ustawia hasła dla kont użytkowników.
PsService	Wylicza i umożliwia kontrolę nad uruchamianiem usług Windows.
PsShutdown	Zamyka system, wylogowuje użytkownika lub zmienia stan zasilania systemu lokalnego i systemów zdalnych.
PsSuspend	Wstrzymuje i wznawia procesy.
Rozdział 8, Narzędzia procesów i diagnostyki	
VMMap	Wyświetla szczegóły wykorzystania pamięci wirtualnej i fizycznej przez procesy.
DebugView	Monitoruje dane wyjściowe debugowania trybu użytkownika i trybu jądra, generowane przez komputer lokalny lub zdalny.
LiveKd	Uruchamia standardowy debuger jądra na migawce uruchomionego systemu lokalnego lub gościa Hyper-V (maszyny wirtualnej) bez konieczności ponownego uruchamianie w trybie debugowania, a dodatkowo umożliwia wykonanie zrzutu pamięci działającego systemu.
ListDLLs	Wyświetla w oknie konsoli informacje o bibliotekach DLL załadowanych w systemie.
Handle	Wyświetla w konsoli informacje o dojściach do obiektów otwartych przez procesy systemu.

Tabela 1-1 Tematyka rozdziałów

Narzędzie	Opis
Rozdział 9, Narzędzia zabezpieczeń	
SigCheck	Weryfikuje podpisy plików, wyświetla wersję i inne informacje o obrazie wykonywalnym, a także odpytuje silniki antywirusowe za pośrednictwem witryny VirusTotal.com
AccessChk	Wyszukuje obiekty, które przyznają uprawnienia określonym użytkownikom lub grupom i udostępnia szczegółowe informacje i przyznanych uprawnieniach.
Sysmon	Monitoruje i zgłasza aktywność systemu; narzędzie nakierowane na identyfikowanie aktywności napastnika.
AccessEnum	Przeszukuje hierarchię plików lub rejestru i identyfikuje miejsca, w których uprawnienia mogły zostać zmienione.
ShareEnum	Wylicza udziały plików i drukarek w sieci oraz informacje, kto ma do nich dostęp.
ShellRunAs	Przywraca możliwość uruchomienia programu przy użyciu poświadczeń innego użytkownika w systemie Windows Vista.
Autologon	Konfiguruje konto użytkownika do automatycznego zalogowania podczas rozruchu systemu.
LogonSessions	Wylicza aktywne sesje logowania Local Security Authority (LSA) na komputerze.
SDelete	Bezpiecznie usuwa pliki lub struktury katalogów i wymazuje dane w zwolnionych obszarach twardego dysku.
Rozdział 10, Narzędzia Active Directory	
AdExplorer	Wyświetla i umożliwia edycję obiektów Active Directory.
AdInsight	Śledzi wywołania API Active Directory Lightweight Directory Access Protocol (LDAP).
AdRestore	Wylicza i przywraca usunięte obiekty Active Directory.
Rozdział 11, Narzędzia pulpitu	
BgInfo	Wyświetla informacje konfiguracyjne komputera jako tło pulpitu (*wallpaper*).
Desktops	Uruchamia aplikacje w oddzielnych pulpitach wirtualnych.
ZoomIt	Powiększa zawartość ekranu i umożliwia tworzenie adnotacji.

Tabela 1-1 Tematyka rozdziałów

Narzędzie	Opis
Rozdział 12, Narzędzia plikowe	
Strings	Przeszukuje pliki pod kątem zawartego w nich tekstu ASCII lub Unicode.
Streams	Identyfikuje systemowe obiekty, które mają alternatywne strumienie danych i umożliwia usunięcie tych strumieni.
Junction	Wylicza i usuwa połączenia katalogów NTFS.
FindLinks	Wylicza twarde łącza NTFS.
DU	Wylicza wielkość logiczną i zajmowanego miejsca dla hierarchii katalogów.
PendMoves	Raportuje operacje plikowe zaplanowane do wykonania podczas następnego uruchomienia systemu.
MoveFile	Planuje operacje plikowe do wykonania podczas następnego uruchomienia systemu.
Rozdział 13, Narzędzia dyskowe	
Disk2Vhd	Tworzy obraz fizycznego dysku jako wirtualny dysk twardy (VHD)
Sync	Zrzuca niezapisane dane z buforów dyskowych na dysk fizyczny.
DiskView	Wyświetla graficzną mapę woluminu (na poziomie klastrów), pozwalając określić, jaki plik znajduje się w określonym klastrze i jakie klastry zajmuje wskazany plik.
Contig	Defragmentuje wskazane pliki lub pokazuje, jak bardzo pofragmentowany jest wybrany plik.
DiskExt	Wyświetla informacje o fragmentach dysku (ekstentach).
LDMDump	Wyświetla szczegółowe informacje o dyskach dynamicznych, odczytywane z bazy danych Logical Disk Manager (LDM).
VolumeID	Zmienia identyfikator woluminu (znany też jako jego numer seryjny).
Rozdział 14, Narzędzia sieciowe	
PsPing	Mierzy czas przebiegu w jedną i w obie strony dla pakietów TCP lub UDP, opóźnienie i pasmo przesyłowe.
TCPView	Wyświetla aktywne punkty końcowe TCP i UDP.
Whois	Zwraca informacje o rejestracji domeny internetowej lub wykonuje odwrotne wyszukiwanie DNS.

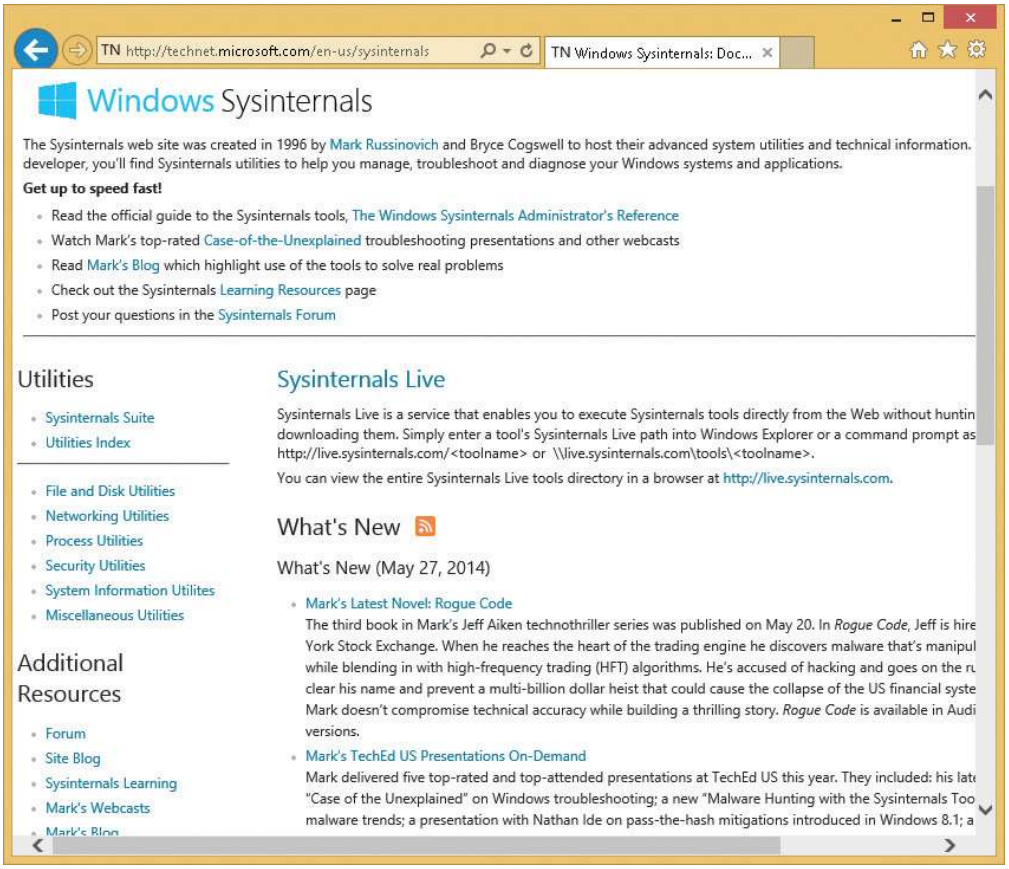
Tabela 1-1 Tematyka rozdziałów

Narzędzie	Opis
Rozdział 15, Narzędzia informacji systemowej	
RAMMap	Udostępnia szczegółowy widok wykorzystania pamięci fizycznej.
RU	Pokazuje użycie miejsca w rejestrze dla wskazanego klucza.
CoreInfo	Zwraca informacje, czy procesor i wersja Microsoft Windows wspiera różne funkcje, takie jak flaga No Execute dla stron pamięci i pokazuje mapowanie procesorów logicznych na rdzenie, podstawki, węzły Non-Uniform Memory Access (NUMA) i grupy procesorów.
WinObj	Wyświetla przestrzeńnazw Windows Object Manager.
LoadOrder	Pokazuje (w przybliżeniu) kolejność, w jakiej system Windows ładuje sterowniki urządzeń i uruchamia usługi.
PipeList	Wylicza nasłuchujące potoki nazwane.
ClockRes	Wyświetla bieżącą, maksymalną i minimalną rozdzielczość zegara systemowego.
Rozdział 16, Różne narzędzia	
RegJump	Uruchamia RegEdit, jednocześnie otwierając wskazaną ścieżkę rejestru.
Hex2Dec	Konwertuje liczby z postaci szesnastkowej na dziesiętną i odwrotnie.
RegDelNull	Wyszukuje i usuwa klucze rejestru z osadzonymi znakami NUL w ich nazwach.
Bluescreen Screen Saver	Wygaszacz ekranu realistycznie symulujący „Blue Screen of Death”.
Ctrl2Cap	Konwertuje naciśnięcie klawisza Caps Lock na naciśnięcie klawisza Control.

Witryna Windows Sysinternals

Najprostszą metodą dotarcia do witryny Sysinternals (rysunek 1-1) jest wpisanie adresu *http://www.sysinternals.com*, który przekierowuje do strony domowej Sysinternals w Microsoft TechNet, aktualnie pod adresem *http://technet.microsoft.com/sysinternals*. Warto zauważyć, że o ile ten drugi adres może się zmienić, strona przekierowująca pozostanie ta sama. Oprócz wszystkich narzędzi z rodziny Sysinternals witryna ta zawiera wiele powiązanych zasobów (albo łącza do nich), takich jak szkolenia,

książki, blogi, artykuły, webcasty, nadchodzące wydarzenia oraz forum społeczności Sysinternals.



Rysunek 1-1 Witryna Windows Sysinternals

Pobieranie narzędzi

Narzędzia Sysinternals można pobierać po jednym na raz, tylko te, których akurat potrzebujemy, albo pobrać cały zbiór w pojedynczym pliku skompresowanym o nazwie SysinternalsSuite.zip. Łącza dostępne na stronie domowej Sysinternals kierują do stron poświęconych poszczególnym narzędziom. Strona Utilities Index wylicza wszystkie narzędzia wraz z łączami do ich pobrania; łącza do kategorii, takich jak File And Disk Utilities (Narzędzia plikowe i dyskowe) lub Networking Utilities (Narzędzia sieciowe) prowadzą do stron, które zawierają tylko odpowiedni podzbiór narzędzi.

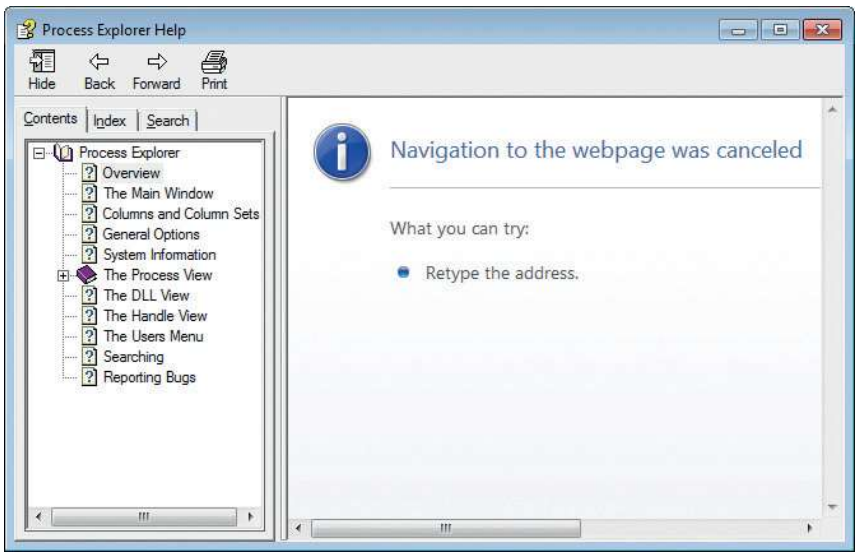
Każde łącze do pobrania prowadzi do pliku skompresowanego (.zip), który zawiera plik wykonywalny (lub wiele plików wykonywalnych), plik tekstowy licencji użytkownika (Eula.txt), a w przypadku niektórych z narzędzi także plik pomocy (.chp lub .hlp).

Uwaga Indywidualne narzędzia PsTool są dostępne do pobrania tylko w zestawach – albo jako zestaw PsTools, albo jako część pełnego Sysinternals Suite.

„Odblokowanie" plików .zip przed wydobyciem plików

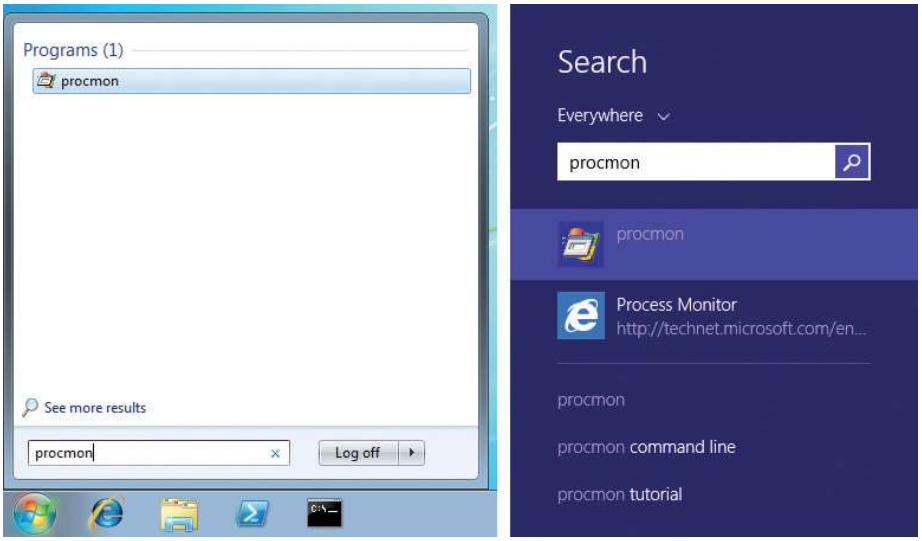
Przed wydobyciem zawartości pobranych plików .zip należy najpierw usunąć znacznik, który nakazuje systemowi Windows traktować tę zawartość jako niezaufaną, co prowadzi do ostrzeżeń i błędów podobnych do pokazanych na rysunkach 1-2 i 1-3. Usługa Windows Attachment Execution Service dodaje alternatywny strumień danych (alternate data stream – ADS) do pliku .zip, sygnalizujący, że plik ten pochodzi z Internetu. Jeśli rozpakujemy pliki przy użyciu Eksploratora Windows, ADS jest propagowany do wszystkich wydobytych plików.

Rysunek 1-2 System Windows wyświetla ostrzeżenie przy otwieraniu plików pobranych z Internetu.



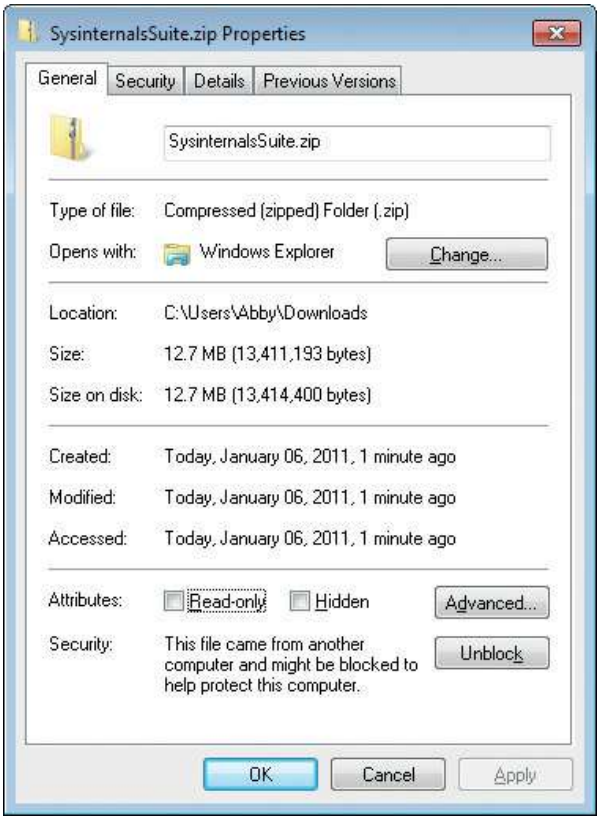
Rysunek 1-3 Skompilowany plik pomocy HTML (CHM) nie może wyświetlić swojej zawartości, gdy jest oznaczony jako pochodzący z Internetu.

Mój współautor, Aaron, nabrał nawyku tworzenia katalogu „C:\Program Files\Sysinternals" i rozpakowywania do niego zawartości Sysinternals Suite, gdzie nie może ona zostać zmodyfikowana przez nieadministracyjnych użytkowników. Następnie dołącza tę lokalizację do systemowej zmiennej środowiskowej `Path`, dzięki czemu można je łatwo uruchomić z dowolnego miejsca, w tym z pola wyszukiwania w menu Start systemu Windows 7 lub z analogicznego pola na ekranie startowym Windows 8.1; obie te lokalizacje zostały pokazane na rysunku 1-4.



Rysunek 1-4 Uruchamianie Procmon za pośrednictwem wyszukiwania w menu Start systemu Windows 7 (po lewej) i na ekranie startowym Windows 8.1 (po prawej).

Jedną metodą usunięcia ADS jest otwarcie okna dialogowego właściwości pliku .zip i kliknięcie przycisku **Unblock** (Odblokuj) w dolnej części karty **General** (Ogólne), pokazanej na rysunku 1-5. Inną metodą jest użycie narzędzia Sysinternals Streams, które opiszę w rozdziale 12, „Narzędzia plikowe".



Rysunek 1-5 Przycisk Unblock pojawiający się w dolnej części okna dialogowego Properties dla pliku pobranego z Internetu

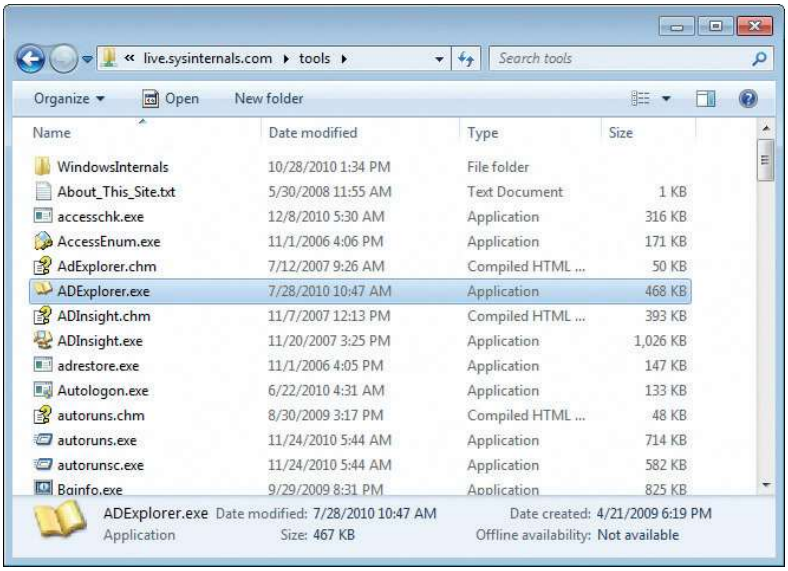
Uruchamianie narzędzi bezpośrednio z sieci Web

Sysinternals Live to usługa, która umożliwia uruchamianie narzędzi Sysinternals bezpośrednio z witryny Web bez konieczności ich wcześniejszego wyszukiwania, pobierania i wypakowywania. Inną zaletą Sysinternals Live jest to, że gwarantuje ona uruchamianie zawsze najnowszych wersji narzędzi.

Aby uruchomić narzędzie przy użyciu usługi Sysinternals Live, należy w pasku adresu Internet Explorer wpisać **http://live.sysinternals.com/*utilityname.exe*** (na przykład **http://live.sysinternals.com/procmon.exe**). Alternatywnie można wyspecyfikować ścieżkę UNC Sysinternals Live w postaci **\\live.sysinternals.com\tools*utilityname.exe***. (Zwróćmy uwagę na dodanie podkatalogu „tools", który nie jest wymagany przy podawaniu adresu URL narzędzia). Na przykład można uruchomić najnowszą wersję Process Monitor, wpisując **\\live.sysinternals.com\tools\procmon.exe**.

Uwaga Składnia UNC dla uruchamiania narzędzi przy użyciu Sysinternals Live wymaga uruchomionej usługi WebClient. W nowszych wersjach Windows usługa ta może nie być skonfigurowana do automatycznego uruchomienia. Bezpośrednie uruchomienie usługi (na przykład poprzez polecenie **net start webclient**) wymaga uprawnień administracyjnych. Usługę można uruchomić pośrednio bez uprawnień administracyjnych, wykonując polecenie **net use \\live.sysinternals.com** w wierszu polecenia lub poprzez przejście do adresu *\\live.sysinternals.com* w Eksploratorze Windows.

Możliwe jest również zamapowanie litery dysku na *\\live.sysinternals.com\tools* lub otwarcie katalogu jako udziału zdalnego w Eksploratorze Windows, co pokazuje rysunek 1-6. Analogicznie można przejrzeć cały katalog Sysinternals Live w przeglądarce, posługując się adresem *http://live.sysinternals.com*.



Rysunek 1-6 Strona Sysinternals Live wyświetlona w Eksploratorze Windows

Pojedynczy obraz wykonywalny

Aby uprościć pakowanie, dystrybucję i przenośność bez konieczności polegania na programach instalacyjnych, wszystkie narzędzia Sysinternals są pojedynczymi, 32-bitowymi obrazami wykonywalnymi, które można bezpośrednio uruchamiać z dowolnej lokalizacji. Zawierają one osadzone dowolne dodatkowe pliki, które mogą być potrzebne jako zasoby, które są rozpakowywane albo do katalogu, w którym znajduje się dany program, albo w przypadku, gdy katalog ten nie jest zapisywalny (na przykład wtedy, gdy znajduje się na nośniku tylko do odczytu, takim jak CD-ROM), w katalogu %TEMP% bieżącego użytkownika. Program usuwa wypakowane pliki, gdy już nie są potrzebne.

Jednym z przykładów wykorzystania tej techniki jest obsługa zarówno 32-, jak i 64-bitowych systemów. W przypadku narzędzi, które wymagają wersji 64-bitowej, aby móc poprawnie działać w 64-bitowym systemie Windows, główny program 32-bit rozpoznaje architekturę procesora, wypakowuje odpowiedni plik binarny x64 lub IA64, po czym go uruchamia. Gdy uruchomimy Process Explorer w systemie x64, zobaczymy Procexp64.exe uruchomiony jako proces potomny procesu Procexp.exe.

Uwaga Jeśli plik programu zostanie wypakowany do %TEMP%, uruchomienie go nie powiedzie się, jeśli wykonywanie z katalogu %TEMP% jest zablokowane, na przykład poprzez reguły AppLocker lub gdy uprawnienia katalogu %TEMP% zostały zmodyfikowane tak, by usunąć uprawnienie Execute.

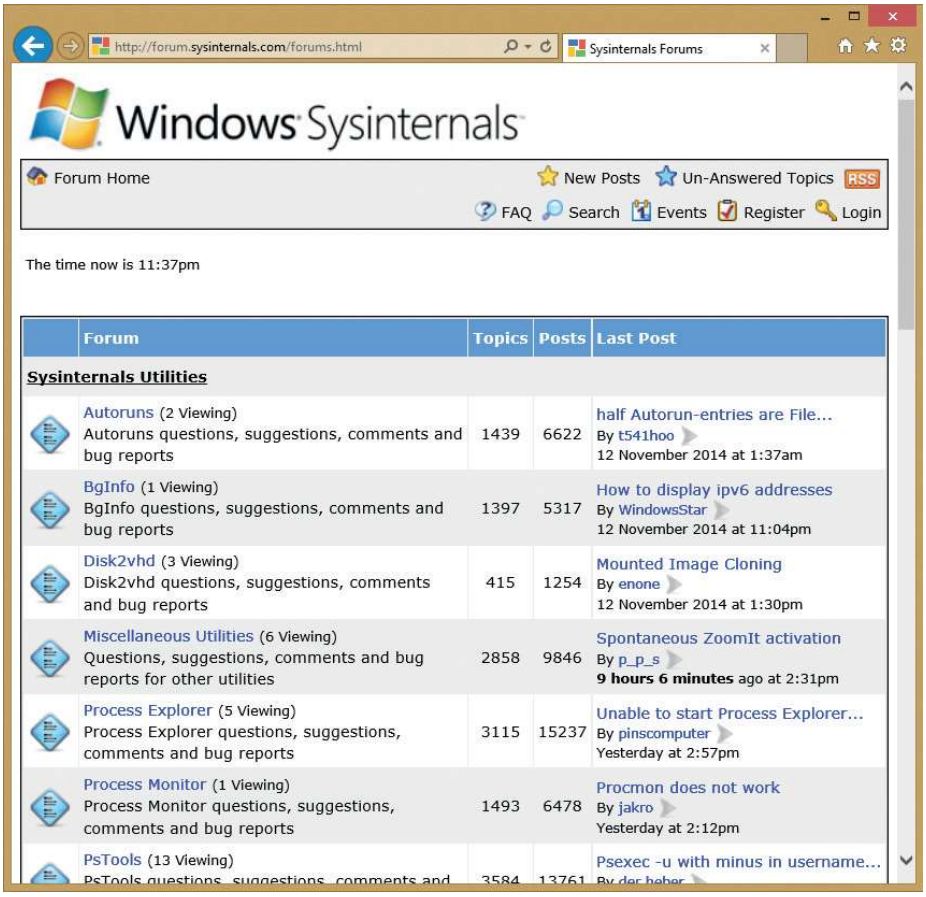
Większość narzędzi Sysinternals, które wykorzystują sterownik trybu jądra, rozpakowują plik sterownika do %SystemRoot%\System32\Drivers, ładują sterownik, po czym usuwają plik. Obraz sterownika pozostaje w pamięci do chwili zamknięcia systemu. Jeśli uruchamiamy nowszą wersję narzędzia, która zawiera zaktualizowany sterownik, załadowanie nowego sterownika może wymagać restartu systemu.

Forum Windows Sysinternals

Forum Windows Sysinternals dostępne pod adresem *http://forum.sysinternals.com* (pokazane na rysunku 1-7) jest pierwszym i najlepszym miejscem, w którym należy szukać odpowiedzi na pytania dotyczące narzędzi Sysinternals i gdzie należy zgłaszać wykryte bugi[1]. Przed zadaniem pytania warto przeszukać istniejące już posty i tematy, aby zobaczyć, czy ktoś inny nie miał już tego samego problemu (i czy został on już rozwiązany). Istnieją oddzielne sekcje poświęcone każdemu z głównych narzędzi Sysinternals, jak również forum, na którym można zgłaszać sugestie nowych funkcjonalności lub narzędzi. Forum również jest miejscem dyskusji na temat wewnętrznych mechanizmów Windows, programowania, rozwiązywania problemów i zwalczania złośliwego oprogramowania.

Wysyłanie wiadomości na forum wymaga rejestracji i zalogowania, ale przy rejestracji wymagane są tylko minimalne informacje. Po zarejestrowaniu można dodatkowo wybrać subskrypcję powiadomień o odpowiedziach na tematy lub nowych postach w określonych sekcjach, a także można wysyłać i odbierać prywatne wiadomości do i od innych uczestników forum.

1 Uwaga do czytelnika polskiego: jak łatwo się domyślić, językiem używanym na forum jest język angielski; nie należy oczekiwać uzyskania odpowiedzi na pytanie zadane w innym języku (przyp. tłum.).



Rysunek 1-7 Forum Windows Sysinternals

Blog Windows Sysinternals

Subskrypcja blogu Sysinternals Site Discussion jest najlepszą metodą otrzymywania powiadomień o nowych narzędziach, aktualizacjach istniejących narzędzi lub innych nowych treściach, które są dostępne w witrynie Sysinternals. Zdecydowanie zalecam utrzymywanie najświeższej wersji narzędzi; wiele zgłaszanych do mnie bugów jest eliminowanych po prostu poprzez zainstalowanie nowszej wersji. Blog witryny dostępny jest pod adresem *http://blogs.technet.com/b/sysinternals*. Choćstrona frontowa wymienia tylko główne aktualizacje narzędzi, w blogu raportowane są wszystkie modyfikacje i aktualizacje, łącznie z najdrobniejszymi.

Blog Marka

Mój własny blog[2] poświęcony jest wewnętrznym mechanizmom Windows, zabezpieczeniom i rozwiązywaniu problemów. Blog zawiera dwie popularne serie artykułów powiązanych z Sysinternals: „The Case of…" (Przypadek…), w którym dokumentuję

2 Jak poprzednio, blogi Sysinternals są prowadzone wyłącznie w języku angielskim (przyp. tłum.).

rozwiązania codziennie zgłaszanych problemów przy użyciu narzędzi Sysinternals; oraz „Pushing the Limits" (Przesuwając granice), w którym opisuję ograniczenia zasobów w systemie Windows, ich monitorowanie i efekty zderzenia się z nimi. Dostęp do blogu zapewnia poniższy URL:

http://blogs.technet.com/b/markrussinovich

Pełną listę postów na moim blogu według tytułów można również znaleźć klikając łącze Mark's Blog na stronie domowej Sysinternals.

Mój współautor Aaron również prowadzi blog na temat Sysinternals, bezpieczeństwa, kompatybilności aplikacji i innych zagadnieńtechnicznych, a ponadto publikuje różne poręczne narzędzia w poniższych witrynach:

http://blogs.msdn.com/b/aaron_margosis

http://blogs.technet.com/b/fdcc

http://blogs.technet.com/b/secguide

Webcasty

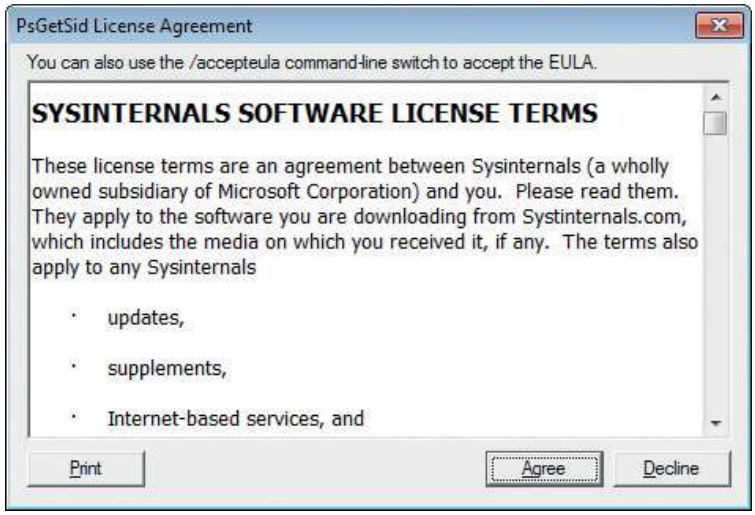
Pełną listę nagrańz moich prezentacji na TechEd i innych konferencjach, dostępnych na żądanie – w tym moje najwyżej klasyfikowane sesje „Case of the Unexplained…", sesje rozwiązywania problemów przy użyciu Sysinternals, moje wywiady dla Channel 9 oraz prowadzone przeze mnie Springboard Virtual Roundtables – można znaleźć po kliknięciu łącza Mark's Webcasts na stronie domowej Sysinternals.

Informacje licencyjne Sysinternals

Narzędzia Sysinternals są bezpłatne. Użytkownik może zainstalować i używać dowolnej liczby kopii oprogramowania na swoich komputerach i komputerach należących do jego firmy. Tym niemniej użycie oprogramowania podlega warunkom licencji, które są wyświetlane przy pierwszym uruchomieniu narzędzia oraz na stronie Software License połączonej ze stroną domową Sysinternals.

End User License Agreement i przełącznik /accepteula

Każde narzędzie wymaga zaakceptowania umowy licencyjnej użytkownika końcowego (End User License Agreement – EULA) przez każdą osobę, która uruchamia dane narzędzie w danym systemie. Za pierwszym razem, gdy użytkownik uruchomi określone narzędzie na danym komputerze – także w przypadku narzędzi konsolowych – wyświetlane jest okno dialogowe EULA podobne do pokazanego na rysunku 1-8. Użytkownik musi kliknąć przycisk Agree (Zgadzam się), zanim narzędzie się uruchomi.



Rysunek 1-8 End User License Agreement dla PsGetSid.

Ponieważ wyświetlenie tego okna dialogowego zakłóca automatyzację i inne nieinteraktywne scenariusze, większość narzędzi Sysinternals akceptuje przełącznik wiersza polecenia **/accepteula** jako poprawne zaakceptowanie umowy licencyjnej. Na przykład poniższe polecenie używa PsExec (opisanego w rozdziale 7) do uruchomienia LogonSessions.exe (opisanego w rozdziale 9) w nieinterakcyjnym kontekście na komputerze *server1*, przy czym przełącznik **/accepteula** dla LogonSessions.exe zabezpiecza przed zablokowaniem go poprzez oczekiwanie na kliknięcie przycisku, które nigdy nie nastąpi:

```
PsExec \\server1 logonsessions.exe /AcceptEula
```

Warto zauważyć, że niektóre narzędzia Sysinternals nie zostały jeszcze zaktualizowane do obsługi przełącznika **/accepteula**. W tych przypadkach konieczne jest ręczne ustawienie flagi sygnalizującej akceptację warunków licencyjnych. Można to zrealizować przy użyciu wiersza polecenia jak poniższy, które tworzy wpis *EulaAccepted* dla kluczy rejestru poszczególnych narzędzi w gałęzi HKEY_CURRENT_USER\Software\Sysinternals rejestru na komputerze *server1*:

```
psexec \\server1 reg add hkcu\software\sysinternals\pendmove /v
eulaaccepted /t reg_dword /d 1 /f
```

Często zadawane pytania na temat licencjonowania Sysinternals

- Ile kopii narzędzi Sysinternals mogę bezpłatnie załadować lub używać na komputerach należących do mojej firmy?

  Nie ma żadnego ograniczenia liczby instalacji i uruchomień oprogramowania na naszych urządzeniach lub komputerach przez nas obsługiwanych.

- Czy mogę rozpowszechniać narzędzia Sysinternals w ramach mojego oprogramowania, na mojej stronie lub w moim czasopiśmie?

  Nie. Firma Microsoft nie oferuje żadnych licencji dystrybucyjnych, nawet jeśli trzecia strona miałaby je rozpowszechniać za darmo. Microsoft zachęca użytkowników do pobierania narzędzi ze swojego centrum pobierania lub uruchamiania ich bezpośrednio z witryny Web, dzięki czemu można zagwarantować, że uzyskają oni najbardziej aktualną wersję narzędzia.

- Czy mogę licencjonować lub ponownie użyć kod źródłowy Sysinternals?

  Nie. Kod źródłowy Sysinternals nie jest już udostępniany do pobrania i nie jest licencjonowany.

- Czy narzędzia Sysinternals nadal będą dostępne bezpłatnie?

  Tak. Firma Microsoft nie ma żadnych planów usunięcia tych narzędzi ani pobierania za nie opłat.

- Czy istnieje pomoc techniczna dla narzędzi Sysinternals?

  Wszystkie narzędzia Sysinternals są oferowane „tak jak są", bez oficjalnego wsparcia ze strony firmy Microsoft. Firma Microsoft utrzymuje natomiast dedykowane forum Sysinternals (*http://forum.sysinternals.com*), na którym można zgłaszać wykryte błędy i proponować nowe funkcjonalności.

ROZDZIAŁ 2

Kluczowe koncepcje systemu Windows

Im więcej ktoś wie o tym, jak działa system Microsoft Windows, tym więcej będzie mógł uzyskać z narzędzi Sysinternals. Rozdział ten zawiera przegląd wybranych koncepcji systemu Windows, które są istotne z punktu widzenia wielu programów Sysinternals; powinno to pomóc w lepszym poznaniu tych, niekiedy niewłaściwie rozumianych zagadnień. Najlepszym i najbardziej wyczerpującym opracowaniem na temat podstawowych komponentów systemu operacyjnego jest *Windows Internals*[1]. Część II tej książki, „Podręcznik użytkowania", może zaoferować co najwyżej skrótowe przedstawienie złożonych zagadnień, takich jak zarządzanie pamięcią w systemie Windows. Ostatecznie tematem tej książki są narzędzia Sysinternals, a nie sam system Windows, zatem nie może ona zawierać wszystkich szczegółów udostępnianych przez *Windows Internals*. Nie ma tu również miejsca na wyczerpujące omówienie architektury Windows, ani na odpowiedzi na podstawowe pytania, które Czytelnik powinien już znać, takich jak „Czym jest rejestr?" lub „Jaka jest różnica pomiędzy TCP a UDP?"

Zagadnienia omówione w tym rozdziale oraz główne narzędzia, których one dotyczą, obejmują:

- Prawa administracyjne oraz sposoby uruchamiania programów przy użyciu tych uprawnień (dotyczy większości narzędzi).
- Procesy, wątki i zadania (Process Explorer, Process Monitor, PsTools, VMMap, ProcDump, TCPView, RAMMap).
- Tryb użytkownika i tryb jądra (Process Explorer, Process Monitor, Autoruns, VMMap, ProcDump, DebugView, LiveKd, TCPView, RAMMap, LoadOrder).
- Dojścia (Process Explorer, Handle).

1 W chwili pisania tych słów najświeższym wydaniem było *Windows Internals*, 6th Edition, części 1 i 2, Mark E. Russinovich, David A. Solomon i Alex Ionescu (Microsoft Press, 2012).

- Izolacja aplikacji (Process Explorer, Process Monitor, AccessChk, WinObj, Sysmon, PsGetSid).
- Stosy wywołań symbole, włącznie z tym, czym jest stos wywołań, czym są symbole i jak konfigurować symbole w narzędziach Sysinternals (Process Explorer, Process Monitor, VMMap).
- Sesje, stacje okien, pulpity i komunikaty okien (Process Explorer, Process Monitor, PsExec, AdInsight, Desktops, LogonSessions, WinObj, RegJump).

Prawa administracyjne

Windows NT od zawsze miały rozbudowany model kontroli dostępu, niezbędny do ochrony wrażliwych zasobów systemowych przed modyfikacją lub ujawnieniem przez nieautoryzowane osoby lub programy. W ramach tego modelu konta użytkowników zasadniczo otrzymują albo uprawnienia administracyjne, albo prawa użytkownika. Administratorzy mają pełny i nieograniczony dostęp do komputera i wszystkich zasobów, podczas gdy użytkownicy (grupa Users) nie mają możliwości dokonywania zmian w ogólnej konfiguracji samego systemu operacyjnego ani uzyskiwania dostępu do danych należących do innych użytkowników. Jednak ze względów historycznych jeszcze niedawno użytkownicy końcowi komputerów Windows często dysponowali dostępem administracyjnym, przez co wiele osób nie zdawało sobie sprawy z tego, że takie rozróżnienie w ogóle istnieje. (Nawet dziś, w najnowszej wersji systemu Windows 10, pierwsze lokalne konto użytkownika tworzone na komputerze jest domyślnie i automatycznie członkiem grupy Administrators).

Uwaga Użytkownicy mogą mieć efektywną kontrolę administracyjną nad komputerem bez jawnego członkostwa w grupie Administrators, jeśli mają możliwość konfigurowania lub kontrolowania oprogramowania uruchamianego w bardziej uprzywilejowanym kontekście zabezpieczeń– na przykład poprzez przyznanie im kontroli nad ogólnosystemowymi lokalizacjami plików lub rejestru, używanymi przez administratorów lub usługi (takie uprawnienia miała grupa Power Users w systemach poprzedzających Windows Vista). Podobny skutek może dać przyznanie użytkownikom „równoważnych administracyjnym" przywilejów, takich jak Debug, Take-Ownership, Restore lub Load Driver, albo włączenie zasady Instalatora Windows Always Install Elevated (Zawsze instaluj z podwyższonymi uprawnieniami), która powoduje, że dowolny pakiet MSI uruchomiony przez dowolnego użytkownika jest wykonywany w kontekście zabezpieczeńkonta System.

W ciągu ostatnich kilku lat organizacje pragnące poprawić poziom zabezpieczeńi zredukować koszty obsługi i pomocy technicznej zaczęły przechodzić na model „nie-admin" dla swoich użytkowników. Wraz z wprowadzeniem w wydaniu Windows Vista mechanizmu kontroli konta użytkownika (User Account Control – UAC) większość