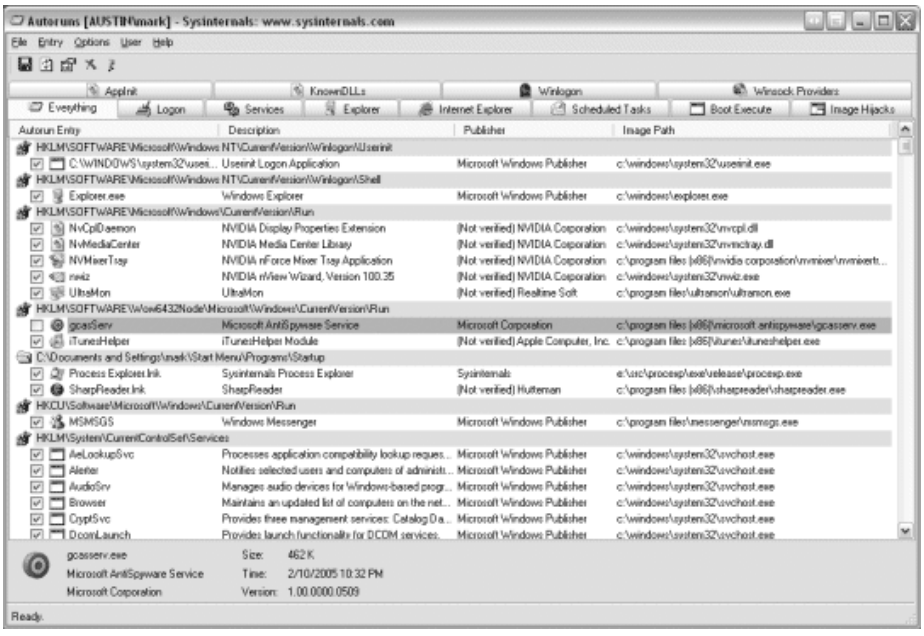
Laboratorium 4

Narzędzia monitorowania składowych systemu operacyjnego

Wśród narzędzi firmy Sysinternals można znaleźć kilka przydatnych aplikacji służących do monitorowania składników ładowanych i wykorzystywanych w pracy systemu operacyjnego (pobierz plik ns.zip). Pierwszym z programów udostępnionych przez firmę Sysinternals jest **Autoruns** pozwalający na szczegółowe sprawdzenie jakie programy lub ich komponenty są skonfigurowane do automatycznego uruchamiania się wraz ze startem systemu operacyjnego. Aplikacja sprawdza nie tylko dostęp do folderu Autostartu, ale także poszczególne klucze systemowego Rejestru (Run, RunOnce i inne), gdzie dosyć często poukrywane są wpisy nie tylko o samych programach, bibliotekach i usługach, lecz także o złośliwych komponentach szpiegujących lub reklamowych instalowanych bez wiedzy użytkowników systemu. Poszczególne zbędne lub złośliwe elementy mogą być w prosty sposób usunięte, co przy zachowaniu odpowiedniej ostrożności powinno spowodować szybsze uruchamianie się systemu oraz jego poprawną pracę. Rysunek 1 przedstawia aplikację Autoruns.



Rys. 1. Aplikacja Autoruns

Kolejne dwa narzędzia **ListDLLs** oraz **Handle** swoje działanie w dużym stopniu opierają na bibliotekach DLL (z ang. *Dynamic Link Library* lub *Dynamic Linked Library* - biblioteka łączona dynamicznie) - w środowisku Windows biblioteka współdzielona

(z ang. *shared library*), która przechowuje implementacje różnych funkcji (podprogramów) programu i/lub zasoby programu).

ListDLLs narzędzie wyświetlające listę wszystkich bibliotek DLL, które aktualnie są załadowane, włączając gdzie są załadowane i numery ich wersji. W starszych wersjach tego narzędzia drukowane były pełne ścieżki dostępu do tych bibliotek.

Handle służy do monitorowania otwartych plików i załadowanych do pamięci DLL-i. Informacje są zbierane na bieżąco. Dla danego procesu program prezentuje jego identyfikator (PID), opis, właściciela użytkownika, który powołał do życia ów proces, priorytet, liczbę otwartych plików i tytuł okna głównego. Natomiast w oknie szczegółów możemy zobaczyć, jakie obiekty są używane przez dany proces.

Handle wyświetla nie tylko pliki, ale także zdarzenia, semafory, porty i klucze rejestru. Jest to doskonałe źródło informacji o tym, jakich zasobów używa dany program. Można w ten sposób sprawdzić, kto używa pliku, którego nie możemy skasować. W przypadku DLL-i program pokazuje adres bazowy, rozmiar pamięci zaalokowany przez bibliotekę, wersję DLL-a i ścieżkę dostępu do jego pliku.

Następnym narzędziem monitorowania procesów jest **PortMon** narzędzie wykorzystywane jest do monitorowania aktywności portu równoległego i szeregowego. Na bieżąco informuje o wszystkich operacjach odczytu i zapisu, jakie zachodzą na portach szeregowych i równoległych serwera. Dla każdego zdarzenia podaje czas jego wystąpienia, proces, który zgłosił żądanie dostępu do portu, rodzaj żądania, identyfikator portu i rezultat wykonanej operacji. PortMon może być używany wówczas, gdy interesuje nas strumień danych wysłanych na port szeregowy bądź równoległy. Co ciekawe, można także monitorować porty odległego serwera. Musi być wtedy na nim uruchomiony PortMon wywołany z opcją "/c".

Process Explorer kolejny program pakietu Sysinternals to rozbudowany i bardzo ceniony w środowiskach administratorów, program umożliwiający kontrolę uruchomionych w systemie procesów. Process Explorer wyświetla szczegółowe informacje o każdym z uruchomionych procesów wraz z podaniem jakie pliki i biblioteki DLL są przez dany proces używane, umożliwia sprawdzanie cyfrowych podpisów plików. Każdy uruchomiony program może zostać uśpiony, wyświetlana jest też lista parametrów z jakimi został uruchomiony. Ponadto, w zasobniku systemowym (tzw. tray) wyświetlane jest użycie mocy procesora i procesu, który pochłania najwięcej mocy obliczeniowej.

Kolejnym narzędziem monitorowania procesów jest pakiet **PsTools** przygotowany przez zespół programistów Sysinternals. W skład pakietu wchodzi 12 narzędzi m.in. (**PsExec**,

PsGetSid, **PsKill**, **PsList**, **PsService**, **PsSuspend**). Zebrane w nim narzędzia działają w trybie tekstowym i umożliwiają analizę zabezpieczeń lokalnego lub zdalnego komputera. PsTools umożliwiają m.in. zdalny dostęp do komputera, do którego udało się już dostać wcześniej przez wykrytą lukę, i rozszerzenie uzyskanych uprawnień. Na przykład po włamaniu do komputera i uzyskaniu statusu lokalnego administratora możesz podjąć próbę uzyskania uprawnień administratora domeny, który akurat jest zalogowany. PsTools pomoże w tym zadaniu, zamykając zdalnie komputery i kończąc procesy.

Pakiet zawiera bardzo ciekawe narzędzie PsExec, które umożliwia osobie z uprawnieniami lokalnego administratora uruchamianie programów na zdalnym komputerze. Zdalne uruchomienie programu wymaga uwierzytelnionego połączenia, np. podania nazwy użytkownika i hasła. Jeśli użytkownik nie posiada odpowiednich uprawnień, musi je zdobyć w inny sposób, PsExec w tym nie pomoże. Parametry programu pozwalają uruchomić na zdalnym komputerze wybrany program. Można również wpisać polecenie psexec \\nazwa_komputera cmd, żeby na zdalnym komputerze uruchomić wiersz poleceń i dopiero z niego uruchamiać programy czy nawigować po zasobach twardego dysku. Należy zwrócić uwagę, że okno wiersza poleceń zdalnego komputera będzie wyświetlane w oknie wiersza poleceń lokalnej maszyny. PsExec ma funkcję kopiowania plików, dzięki czemu można przenieść potrzebny program z lokalnego komputera, jeśli nie ma go w zdalnym.

Kolejne przydatne narzędzia to PsList i PsKill. Pierwsze wyświetla listę działających procesów na zdalnym komputerze, drugie umożliwia zakończenie wybranego procesu na zdalnym komputerze. Pakiet PsTools jest stale rozwijany. Przydaje się nie tylko do testowania zabezpieczeń, ale również w codziennej pracy administratora.

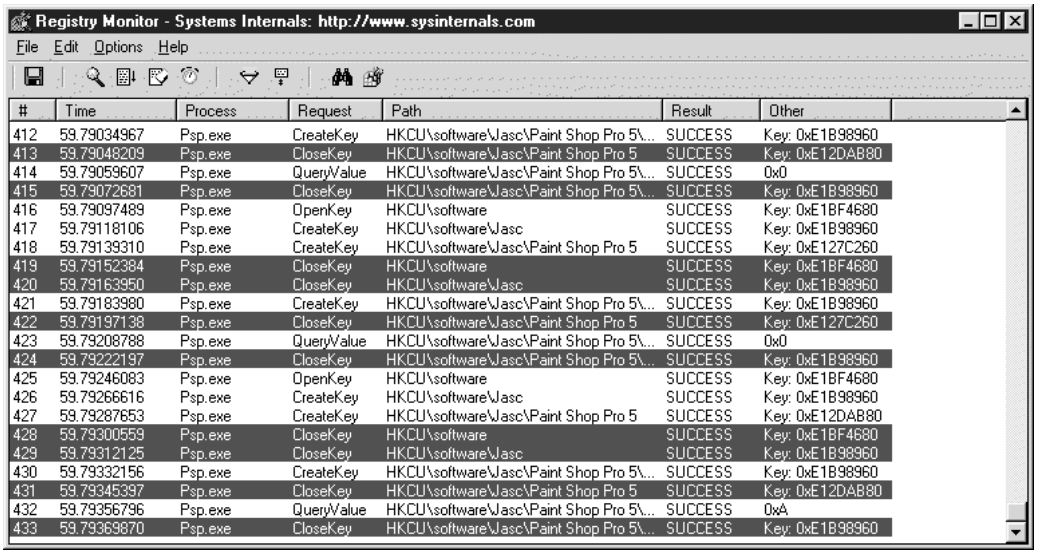
Pełny zestaw narzędzi PsTools do zdalnego zarządzania zasobami komputera to:

- PsExec - zdalne wykonywanie komend,
- PsFile - pokazuje otwarte pliki,
- PsGetSid - pokazuje SID komputera oraz użytkownika,
- PsInfo - szczegółowe informacje o systemie,
- PsKill - zabijanie procesów po PID,
- PsList - dokładne informacje o uruchomionych procesach,
- PsLoggedOn - zobacz jaki użytkownik jest obecnie zalogowany,
- PsLogList - zrzut dziennika podglądu zdarzeń,
- PsPasswd - zmiana haseł użytkowników lokalnych,
- PsService - administracja usługami,

- PsShutdown - restartowanie i wyłączanie zdalnych maszyn,
- PsSuspend - wstrzymywanie procesów,

Kolejne narzędzie o nazwie **ShellRunas**, zaprezentowano w lutym 2008 roku aplikacja ta pomaga uruchamiać programy z poziomu dowolnego użytkownika za pomocą menu kontekstowego.

Ostatnim programem monitorującym procesy naszego systemu jest narzędzie **RegMon** które monitoruje na bieżąco zapis i odczyt z rejestru systemowego. Każda próba zapisu/odczytu jest wychwytywana przez program, a szczegóły operacji są wyświetlane na liście w oknie głównym aplikacji. Przedstawiane są takie informacje, jak nazwa procesu (plik wykonywalny), typ operacji (otwarcie/zamknięcie klucza, odczyt i zapis danych), klucz rejestru, w którym dana operacja miała miejsce, wynik operacji i inne. Aplikację RegMon przedstawia rysunek 2.



#	Time	Process	Request	Path	Result	Other
412	59.79034967	Psp.exe	CreateKey	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	Key: 0xE1B98960
413	59.79048209	Psp.exe	CloseKey	HKCU\software\Jasc\Paint Shop Pro 5	SUCCESS	Key: 0xE12DAB80
414	59.79059607	Psp.exe	QueryValue	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	0x0
415	59.79072681	Psp.exe	CloseKey	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	Key: 0xE1B98960
416	59.79097489	Psp.exe	OpenKey	HKCU\software	SUCCESS	Key: 0xE1BF4680
417	59.79118106	Psp.exe	CreateKey	HKCU\software\Jasc	SUCCESS	Key: 0xE1B98960
418	59.79139310	Psp.exe	CreateKey	HKCU\software\Jasc\Paint Shop Pro 5	SUCCESS	Key: 0xE127C260
419	59.79152384	Psp.exe	CloseKey	HKCU\software	SUCCESS	Key: 0xE1BF4680
420	59.79163950	Psp.exe	CloseKey	HKCU\software\Jasc	SUCCESS	Key: 0xE1B98960
421	59.79183980	Psp.exe	CreateKey	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	Key: 0xE1B98960
422	59.79197138	Psp.exe	CloseKey	HKCU\software\Jasc\Paint Shop Pro 5	SUCCESS	Key: 0xE127C260
423	59.79208788	Psp.exe	QueryValue	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	0x0
424	59.79222197	Psp.exe	CloseKey	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	Key: 0xE1B98960
425	59.79246083	Psp.exe	OpenKey	HKCU\software	SUCCESS	Key: 0xE1BF4680
426	59.79266616	Psp.exe	CreateKey	HKCU\software\Jasc	SUCCESS	Key: 0xE1B98960
427	59.79287653	Psp.exe	CreateKey	HKCU\software\Jasc\Paint Shop Pro 5	SUCCESS	Key: 0xE12DAB80
428	59.79300559	Psp.exe	CloseKey	HKCU\software	SUCCESS	Key: 0xE1BF4680
429	59.79312125	Psp.exe	CloseKey	HKCU\software\Jasc	SUCCESS	Key: 0xE1B98960
430	59.79332156	Psp.exe	CreateKey	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	Key: 0xE1B98960
431	59.79345397	Psp.exe	CloseKey	HKCU\software\Jasc\Paint Shop Pro 5	SUCCESS	Key: 0xE12DAB80
432	59.79356796	Psp.exe	QueryValue	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	0xA
433	59.79369870	Psp.exe	CloseKey	HKCU\software\Jasc\Paint Shop Pro 5\...	SUCCESS	Key: 0xE1B98960

Rys. 2. Działanie aplikacji RegMon

Z dodatkowych właściwości programu można wymienić:

- możliwość zatrzymania i wznowienia monitorowania w dowolnym momencie,
- zaawansowane filtrowanie - wybór operacji, które mają być monitorowane, wyświetlanie tylko elementów zawierających podany tekst, ukrywanie elementów zawierających podany tekst,
- wyróżnianie kolorem elementów zawierających podany tekst,
- możliwość zapisania szczegółowego raportu do pliku tekstowego.