

System operacyjny

Marcin Szeliga
marcin@wss.pl



Microsoft®
Most Valuable
Professional

Agenda

■ Wprowadzenie

- Model bezpieczeństwa systemu operacyjnego

■ Zagrożenia

- Lista TOP 5 wg SANS
- Wirusy, robaki
- Rootkity

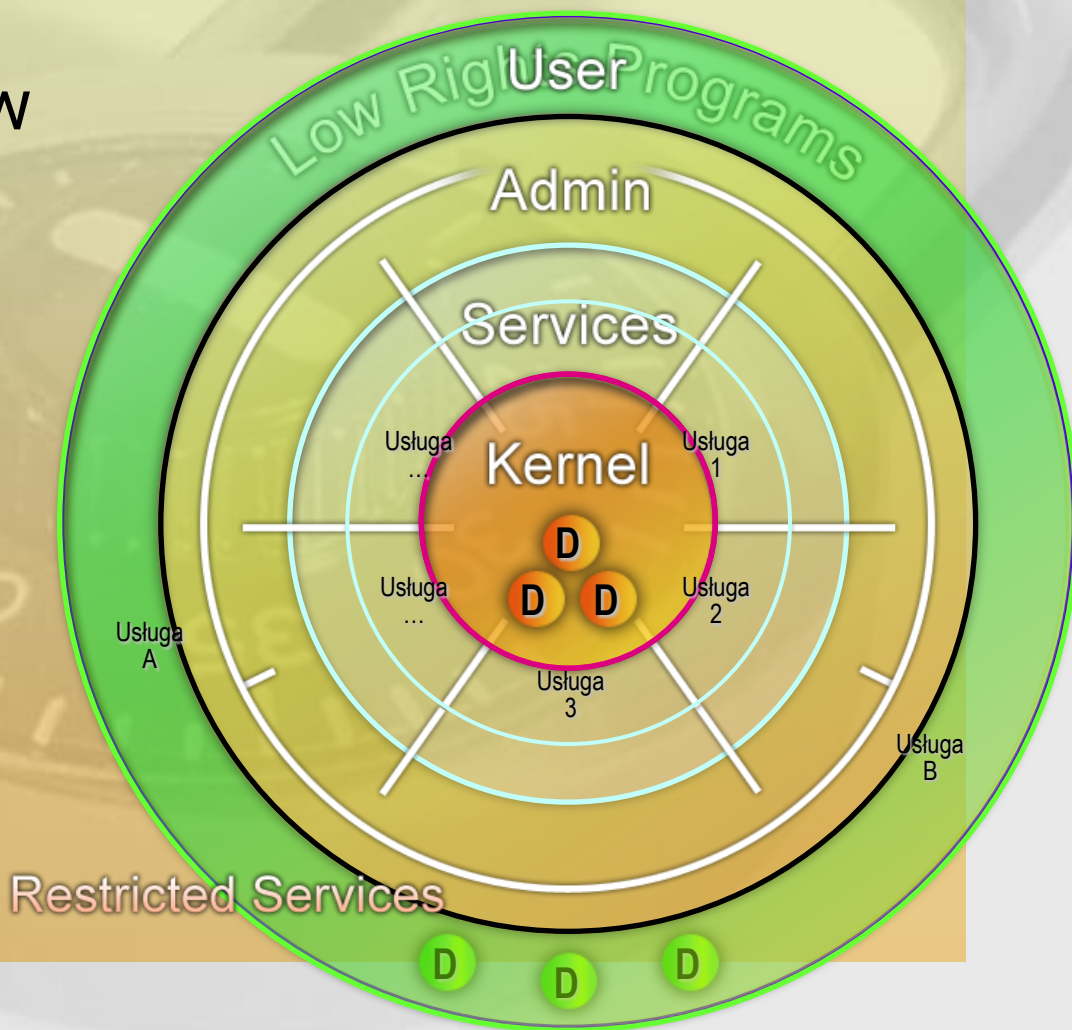
■ Wbudowane zabezpieczenia

- Kontrola konta użytkownika

■ Narzędzia dodatkowe

Model bezpieczeństwa systemu operacyjnego

- Ograniczenie rozmiaru warstw wysokiego ryzyka
- Segmentacja usług
- Większa liczba warstw



D Sterowniki jądra

D Sterowniki trybu użytkownika

Wzmacnianie usług systemowych

- Usługi systemu Windows stały się dużym polem do ataków ze względu na ich uprawnienia i na to, że są prawie zawsze włączone
- Ulepszenia:
 - Identyfikator zabezpieczeń SID (przypisywany do każdej usługi osobno) jest rozpoznawany na listach ACL, dzięki czemu usługi mogą chronić swoje zasoby
 - Zasady zapory sieciowej uniemożliwiają usługom uzyskiwanie dostępu do sieci na podstawie list ACL i identyfikatorów SID
 - Zbędne uprawnienia (w odniesieniu do poszczególnych usług) zostały odrzucone
 - Przejście od trybu LocalSystem do trybu LocalService lub NetworkService, gdy to było możliwe
 - Zastosowanie do procesów usług tokenów o ograniczonym prawie zapisu (write-restricted tokens)

Izolacja sesji 0

Sesja 2

Aplikacja 4
Aplikacja 5



Sesja 0

Usługa 1
Usługa 2

Sesja 1

Aplikacja 1
Aplikacja 2
Aplikacja 3



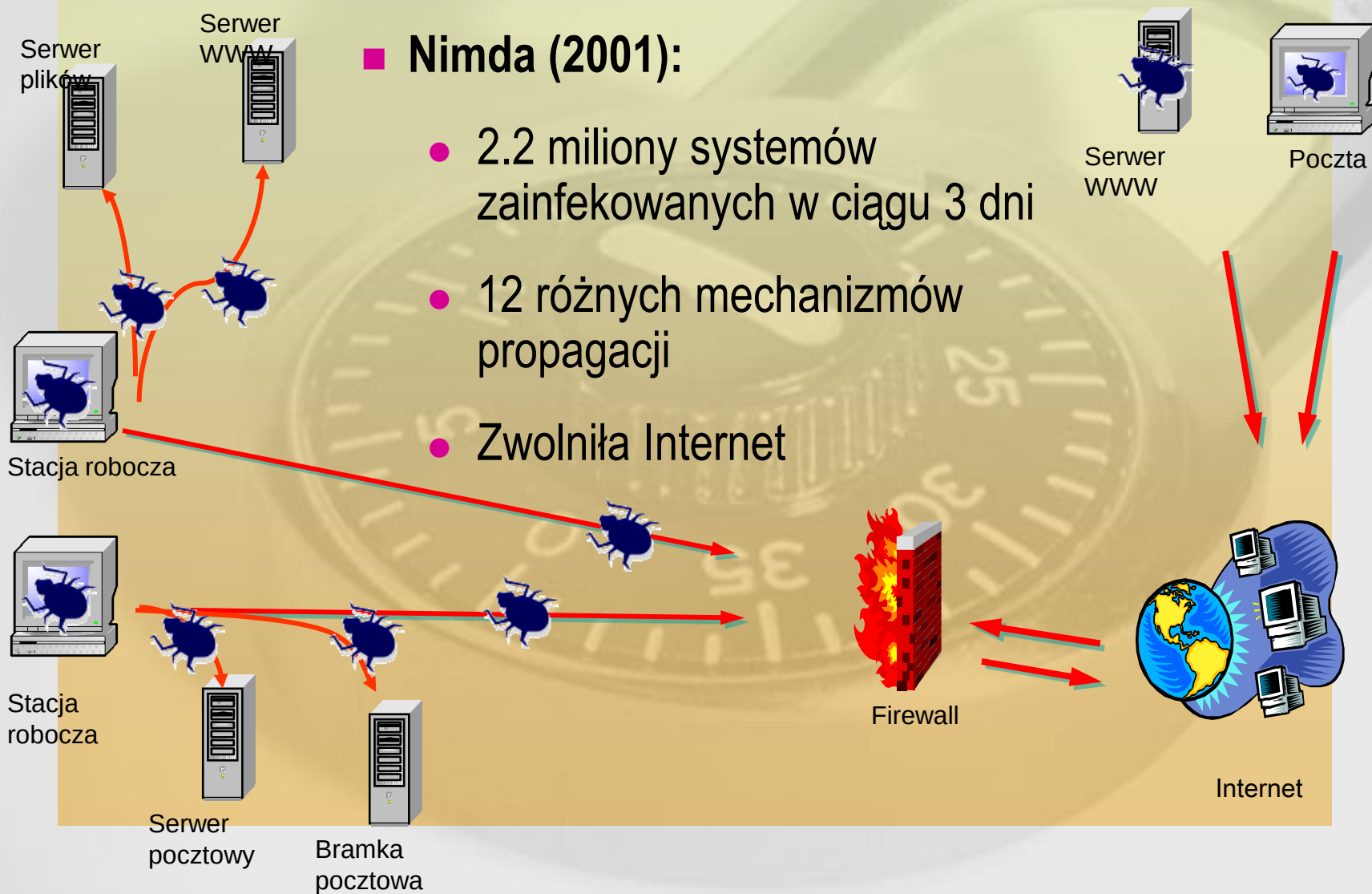
Zagrożenia – Lista TOP 5 wg SANS

- **Internet Explorer w wersjach <7**
 - Skrypty, kontrolki ActiveX, aplety Java, Phishing
- **Biblioteki systemowe**
 - Np. Graphics Rendering Engine
- **Pakiet Microsoft Office**
 - Exploity typu zero-day
- **Usługi systemowe**
- **Niewłaściwe konfiguracja**
 - Słabe hasła (w tym kont usług systemowych)
 - Pusta sesja, włączone konto gościa

Zagrożenia - wirusy

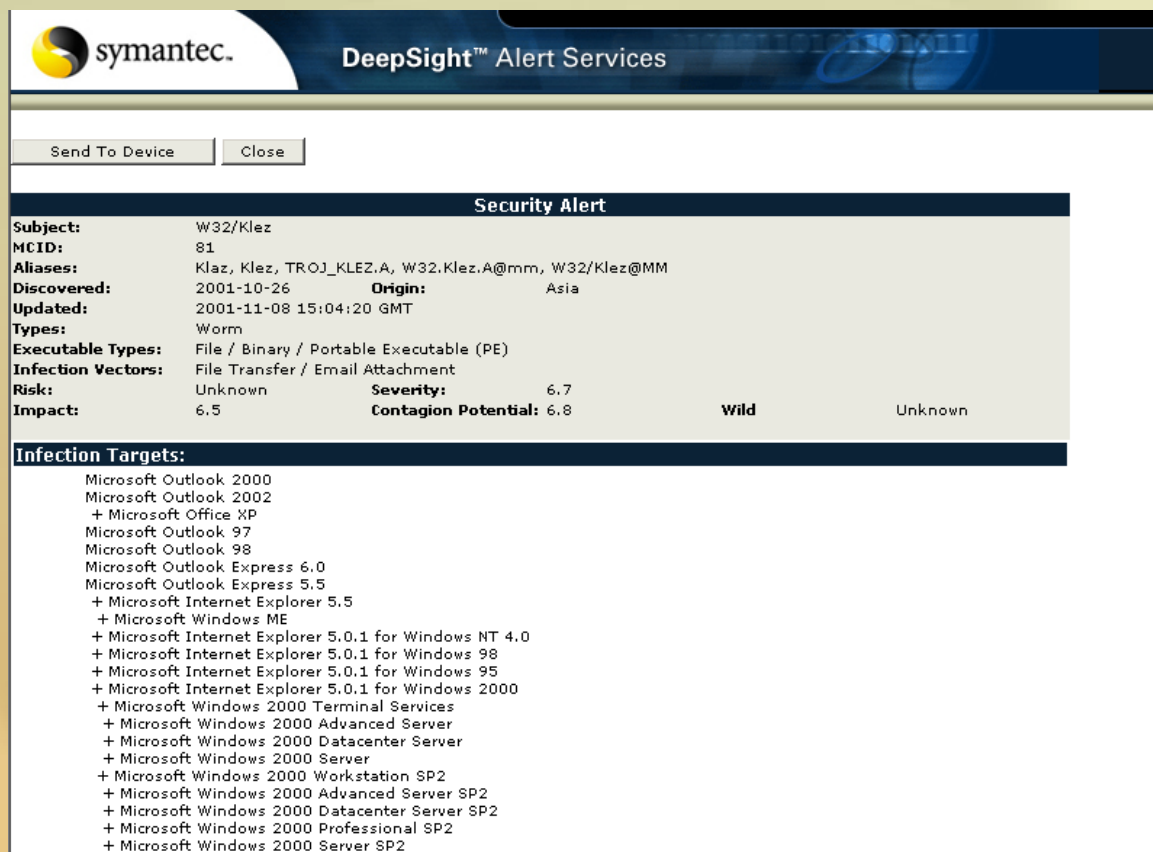
■ Nimda (2001):

- 2.2 miliony systemów zainfekowanych w ciągu 3 dni
- 12 różnych mechanizmów propagacji
- Zwolniła Internet



Zagrożenia - wirusy

KLEZ (2002) dotarł wszędzie w 2 i pół godziny



The screenshot shows a Symantec DeepSight Alert Services window. At the top, there is a Symantec logo and the text "DeepSight™ Alert Services". Below this, there are two buttons: "Send To Device" and "Close". The main content area is titled "Security Alert" and contains the following information:

Subject:	W32/Klez		
MCID:	81		
Aliases:	Klaz, Klez, TROJ_KLEZ.A, W32.Klez.A@mm, W32/Klez@MM		
Discovered:	2001-10-26	Origin:	Asia
Updated:	2001-11-08 15:04:20 GMT		
Types:	Worm		
Executable Types:	File / Binary / Portable Executable (PE)		
Infection Vectors:	File Transfer / Email Attachment		
Risk:	Unknown	Severity:	6.7
Impact:	6.5	Contagion Potential:	6.8
		Wild	Unknown

Below the table, there is a section titled "Infection Targets:" which lists the following targets:

- Microsoft Outlook 2000
- Microsoft Outlook 2002
- + Microsoft Office XP
- Microsoft Outlook 97
- Microsoft Outlook 98
- Microsoft Outlook Express 6.0
- Microsoft Outlook Express 5.5
- + Microsoft Internet Explorer 5.5
- + Microsoft Windows ME
- + Microsoft Internet Explorer 5.0.1 for Windows NT 4.0
- + Microsoft Internet Explorer 5.0.1 for Windows 98
- + Microsoft Internet Explorer 5.0.1 for Windows 95
- + Microsoft Internet Explorer 5.0.1 for Windows 2000
- + Microsoft Windows 2000 Terminal Services
- + Microsoft Windows 2000 Advanced Server
- + Microsoft Windows 2000 Datacenter Server
- + Microsoft Windows 2000 Server
- + Microsoft Windows 2000 Workstation SP2
- + Microsoft Windows 2000 Advanced Server SP2
- + Microsoft Windows 2000 Datacenter Server SP2
- + Microsoft Windows 2000 Professional SP2
- + Microsoft Windows 2000 Server SP2

Zagrożenia - wirusy

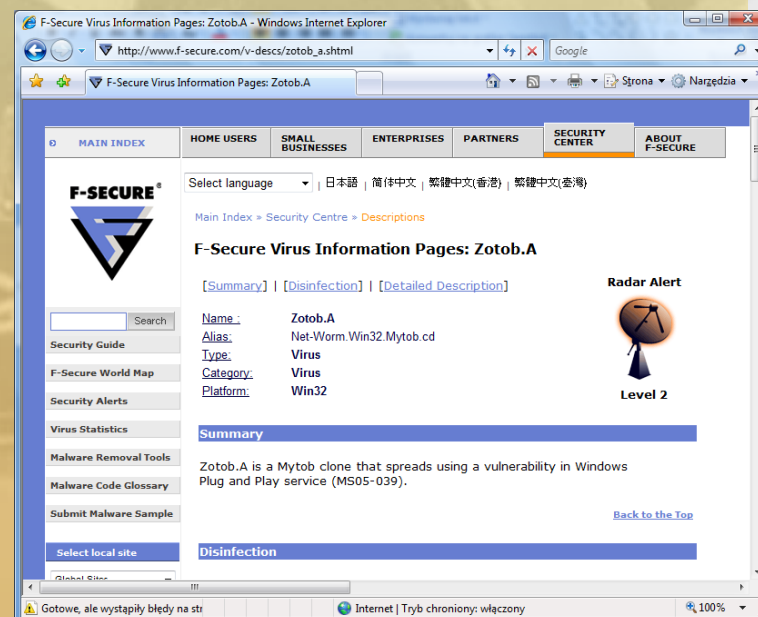
- **SLAMMER (2003) potrzebował tylko 10 minut**
 - Ponad 90% podatnych na atak serwerów SQL zostało zainfekowane w ciągu 10 minut.
 - Podwojenie liczby zainfekowanych maszyn następowało co 8.5 sekundy (w przypadku robaka CodeRed było to 37 minut)
 - Z powodu zalania sieci m.in. odwołano loty i wyłączono bankomaty



Zagrożenia - Wirusy

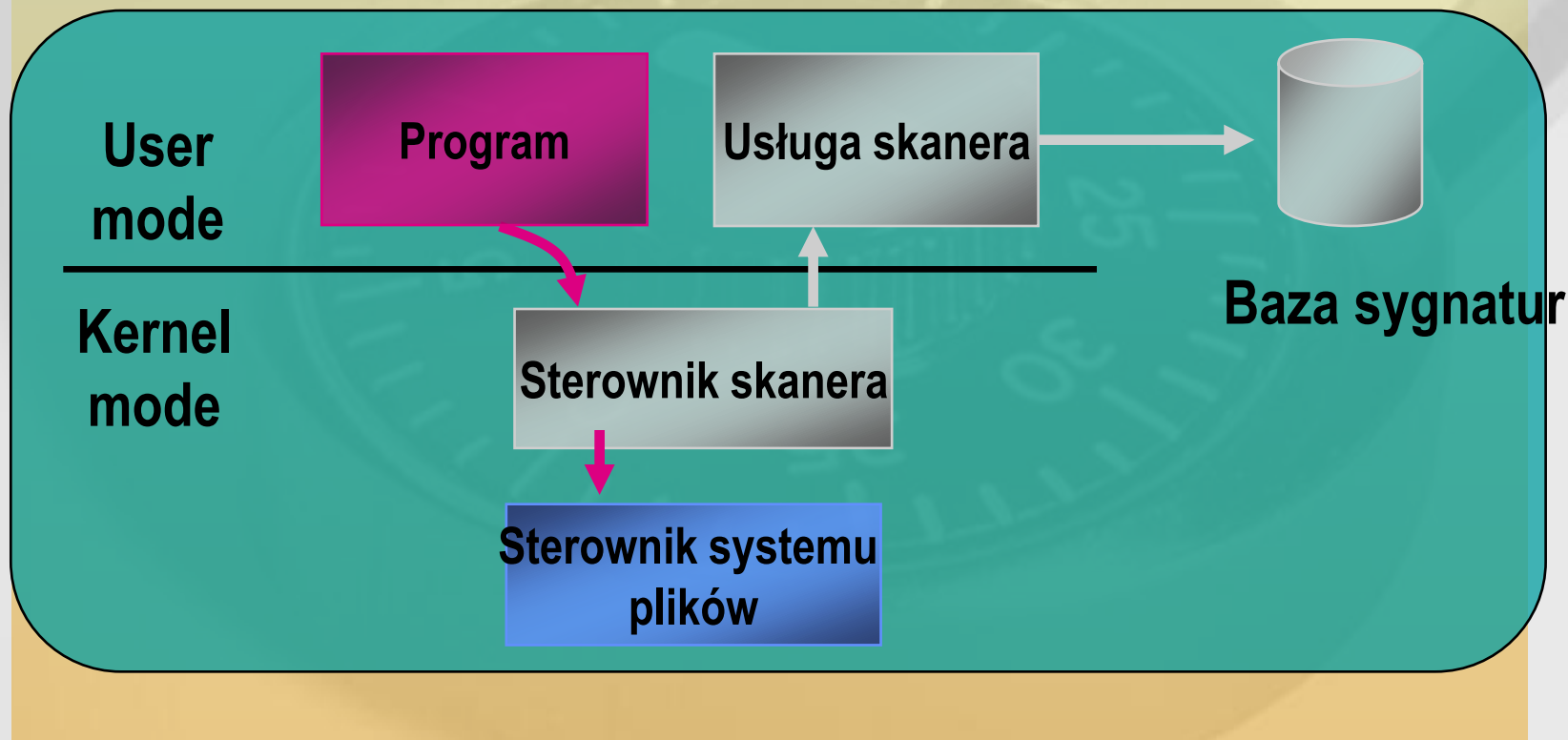
- **ZOTOB (2005):**

- Został napisany na zamówienie przez Turka i Marokańczyka
- Sparaliżował CNN live
- A następnie wybrane firmy, głównie banki



Zagrożenia - wirusy

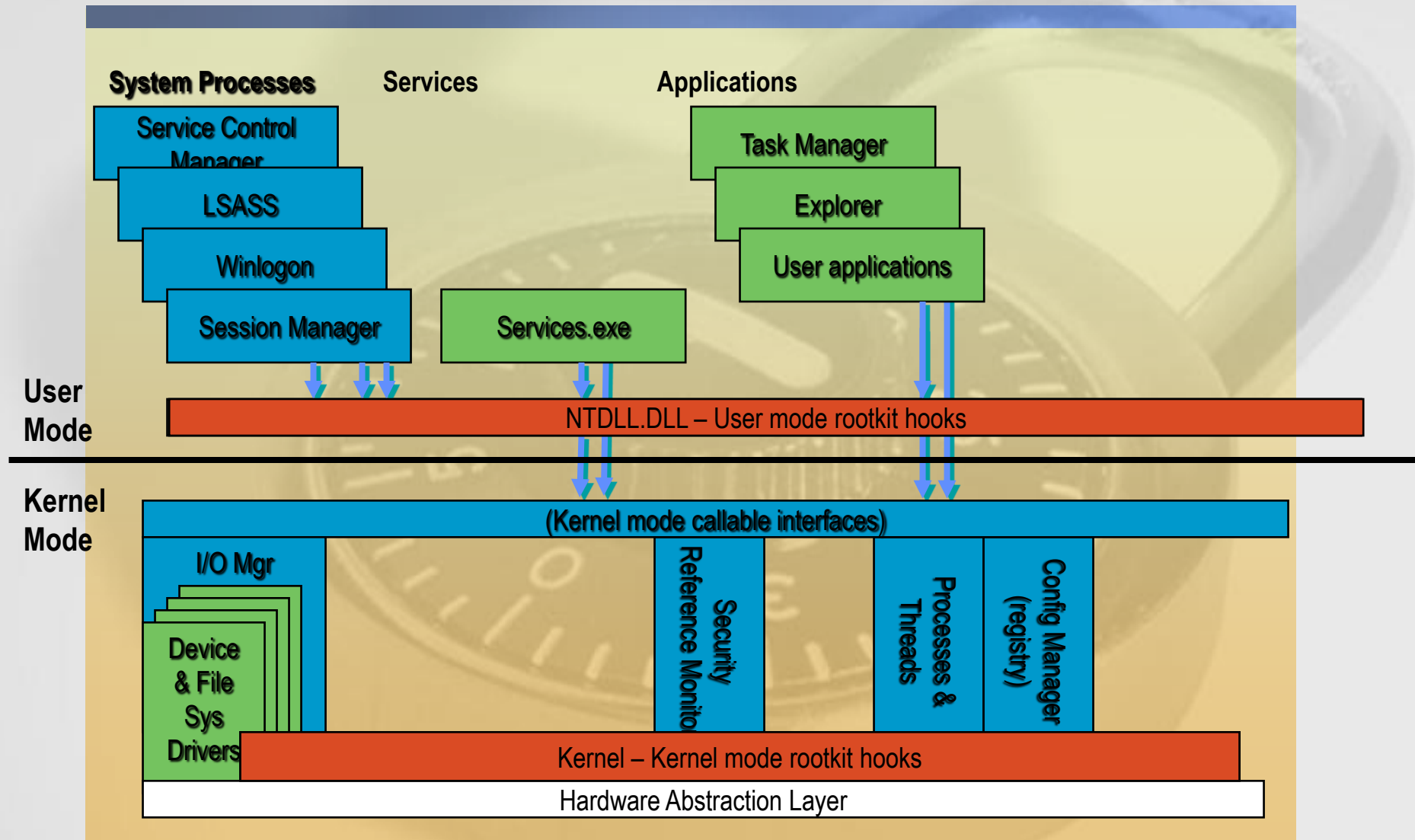
- Programy antywirusowe bazują na sygnaturach
- Przechwytyją operacje I/O



Zagrożenia - Rootkity

- **Rootkit** - program który ma ukryć zmiany w działaniu systemu operacyjnego, nowe lub zmienione pliki, otwarte porty, klucze rejestru, konta użytkowników, itp.
 - Używany do ukrycia przed użytkownikami i administratorami ataku, wewnętrznych mechanizmów systemowych lub dodatkowych usług czy programów (Sony)
- **Mogą działać w trybie użytkownika lub jądra**
- **Pierwszy rootkit (1994) – zastępował narzędzia systemu SunOS (ls, pc, itd.)**
- **Pierwszy wirus na komputery PC (Brain) ukrywał swoją obecność**

Zagrożenia - Rootkity



Zagrożenia – Rootkity (API użytkownika)

- Zmieniają działanie (filtrują) API użytkownika



- Zalety: Nie wymagają uprawnień administracyjnych
- Wady: Można je obejść bezpośrednio wywołując API jądra systemu
- Przykłady: HackerDefender, Afx

Zagrożenia – Rootkity (API jądra systemu)

- Zmieniają działania (filtrują) API jądra systemu



Zagrożenia – Rootkity (modyfikacja jądra systemu)

- **Modyfikują działanie systemu**

- Ukrywają swoje aktywne procesy
- Ale nadal są one wykonywane przez scheduler systemowy

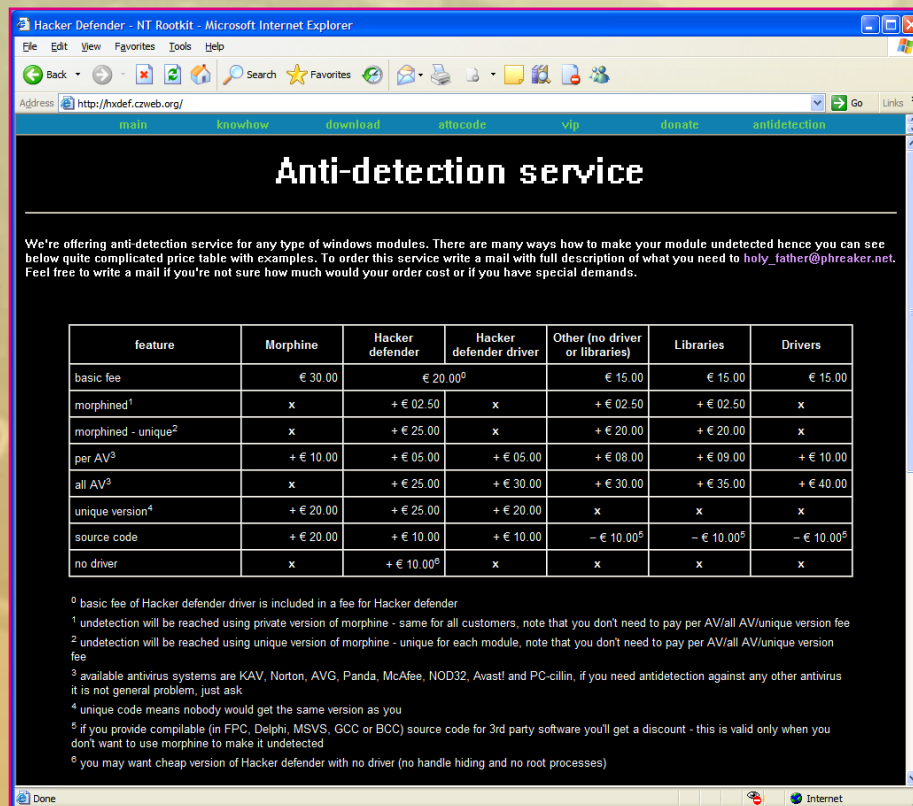


- **Zalety: Ogromne możliwości**
- **Wady: Wymagają uprawnień administratora, znane sposoby wykrycia**
- **Przykład: FU**

Zagrożenia - Rootkity

■ Ogólnodostępne:

- W sieci można znaleźć narzędzia do ich tworzenia
- Gotowe rootkity
- Można je też po prostu kupić



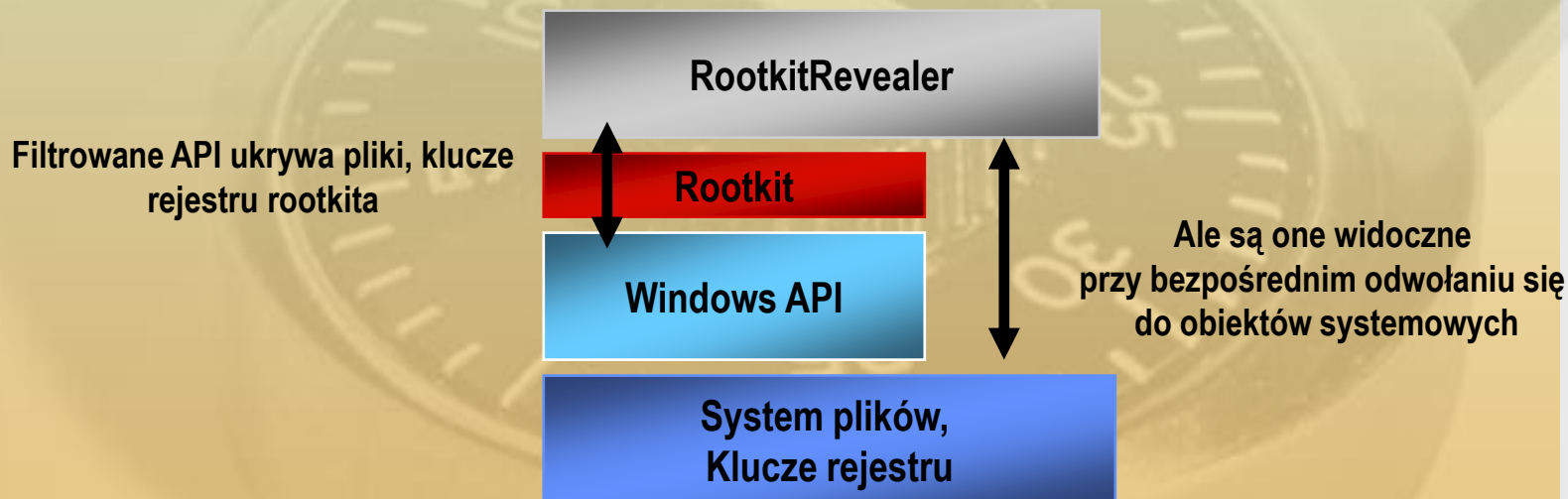
The screenshot shows a web browser window titled "Hacker Defender - NT Rootkit - Microsoft Internet Explorer". The address bar shows "http://hxdef.cxweb.org/". The website has a navigation bar with links: main, knowhow, download, altcode, vip, donate, and antidetection. The main content area is titled "Anti-detection service" and contains a paragraph about the service. Below this is a table with 7 columns: feature, Morphine, Hacker defender, Hacker defender driver, Other (no driver or libraries), Libraries, and Drivers. The table lists various features and their associated costs in Euros. Below the table are footnotes explaining the pricing details.

feature	Morphine	Hacker defender	Hacker defender driver	Other (no driver or libraries)	Libraries	Drivers
basic fee	€ 30.00	€ 20.00 ⁰		€ 15.00	€ 15.00	€ 15.00
morphined ¹	x	+ € 02.50	x	+ € 02.50	+ € 02.50	x
morphined - unique ²	x	+ € 25.00	x	+ € 20.00	+ € 20.00	x
per AV ³	+ € 10.00	+ € 05.00	+ € 05.00	+ € 08.00	+ € 09.00	+ € 10.00
all AV ³	x	+ € 25.00	+ € 30.00	+ € 30.00	+ € 35.00	+ € 40.00
unique version ⁴	+ € 20.00	+ € 25.00	+ € 20.00	x	x	x
source code	+ € 20.00	+ € 10.00	+ € 10.00	- € 10.00 ⁵	- € 10.00 ⁵	- € 10.00 ⁵
no driver	x	+ € 10.00 ⁶	x	x	x	x

⁰ basic fee of Hacker defender driver is included in a fee for Hacker defender
¹ undetection will be reached using private version of morphine - same for all customers, note that you don't need to pay per AV/all AV/unique version fee
² undetection will be reached using unique version of morphine - unique for each module, note that you don't need to pay per AV/all AV/unique version fee
³ available antivirus systems are KAV, Norton, AVG, Panda, McAfee, NOD32, Avast! and PC-cillin, if you need antidetection against any other antivirus it is not general problem, just ask
⁴ unique code means nobody would get the same version as you
⁵ if you provide compilable (in FPC, Delphi, MSVS, GCC or BCC) source code for 3rd party software you'll get a discount - this is valid only when you don't want to use morphine to make it undetected
⁶ you may want cheap version of Hacker defender with no driver (no handle hiding and no root processes)

Zagrożenia - Rootkity

- O wiele łatwiej jest zapobiegać ich instalacji niż je wykryć
 - Nie filtrują całego API, mają zauważalne efekty uboczne i nie działają, gdy system jest wyłączony



- Automatyczne usunięcie jest z reguły niemożliwe

Zagrozenia - Rootkity

- Rootkir Revealer
- Black Light

The image shows two overlapping windows from a Windows XP desktop. The background window is the 'F-Secure BlackLight Beta' application, which is in the 'Step 1 - Scan for hidden items' phase. It displays scan targets (Hidden processes, Hidden files and folders) and a status message: 'Scan complete. 3 hidden items found'. A smaller, foreground window of the same application is open, showing a list of processes. The list includes: 7 lsass.exe (PID 272), 8 svchost.exe (PID 440), 9 svchost.exe (PID 484), 10 spoolsv.exe (PID 532), 11 hxdet100.exe (PID 584, highlighted), 12 syslogd_service.exe (PID 596), 13 lsrv.exe (PID 620), 14 regsv.exe (PID 688), 15 MSTask.exe (PID 728), and 16 siswsv.exe (PID 788). The total number of processes is 37. An 'OK' button is at the bottom. Overlaid on the right is the 'Windows Task Manager' window, showing the 'Processes' tab. It lists various system processes with columns for Image Name, PID, CPU, CPU Time, and Mem Usage. The processes listed include ATKOSD.exe, blbeta.exe, CSRSS.EXE, dfssvc.exe, explorer.exe, gg.exe, HControl.exe, HSFPCWCFG.EXE, inetinfo.exe, internat.exe, LLSSRV.EXE, LSASS.EXE, msdtc.exe, mstask.exe, regsv.exe, SERVICES.EXE, sistray.exe, siswsv.exe, and SiWake.exe. The status bar at the bottom of Task Manager shows 'Processes: 36', 'CPU Usage: 0%', and 'Mem Usage: 168304K / 2370228K'.

F-Secure BlackLight Beta

Step 1 - Scan for hidden items

Scan targets:
Hidden processes
Hidden files and folders

Status:
Scan complete.
3 hidden items found

F-Secure BlackLight Beta

#	Process name	PID
7	lsass.exe	272
8	svchost.exe	440
9	svchost.exe	484
10	spoolsv.exe	532
11	hxdet100.exe	584
12	syslogd_service.exe	596
13	lsrv.exe	620
14	regsv.exe	688
15	MSTask.exe	728
16	siswsv.exe	788

Total number of processes: 37

Windows Task Manager

Image Name	PID	CPU	CPU Time	Mem Usage
ATKOSD.exe	1592	00	0:00:00	2 704 K
blbeta.exe	1664	00	0:00:01	8 248 K
CSRSS.EXE	212	00	0:00:00	2 220 K
dfssvc.exe	980	00	0:00:00	1 756 K
explorer.exe	1028	00	0:00:05	4 256 K
gg.exe	1360	00	0:00:00	10 856 K
HControl.exe	1300	00	0:00:00	2 884 K
HSFPWCFG.EXE	1328	00	0:00:00	1 884 K
inetinfo.exe	1024	00	0:00:01	10 288 K
internat.exe	1344	00	0:00:00	1 812 K
LLSSRV.EXE	620	00	0:00:00	2 336 K
LSASS.EXE	272	00	0:00:00	5 684 K
msdtc.exe	1052	00	0:00:00	5 864 K
mstask.exe	728	00	0:00:00	3 492 K
regsv.exe	688	00	0:00:00	1 084 K
SERVICES.EXE	260	00	0:00:03	7 080 K
sistray.exe	1416	00	0:00:00	2 424 K
siswsv.exe	788	00	0:00:00	1 112 K
SiWake.exe	1404	00	0:00:00	3 708 K

Processes: 36 CPU Usage: 0% Mem Usage: 168304K / 2370228K

■ System Virginty Verifier

The screenshot displays three overlapping command prompt windows on a Windows XP desktop. The background window shows the execution of the 'svv' command with various options. The middle window shows the results of the 'svv check' command, indicating a 'WARNING: Service Table redirection detected' and listing several files as 'suspected'. The foreground window shows the results of the 'svv check' command, indicating a 'SYSTEM INFECTION LEVEL: 5' and listing several files as 'suspected'.

Background Window (C:\WINDOWS\system32\cmd.exe):

```

C:\WINDOWS\system32\cmd.exe
svv <command> [options] [/l <altKernelModuleName>]
command is one of the following:
check      - check system virginity
fix        - try to fix suspected modifications (disinfection)
report     - generate report

```

Middle Window (C:\WINDOWS\system32\cmd.exe):

```

C:\WINDOWS\system32\cmd.exe
already beneath target verdict level, nothing to be fixed!
C:\Documents and Settings\kravietz\My Documents\Szkolenie - WYKRYWANIE\wykrywani
le_programy\Rootkit detection\SUU>svv check /a
WARNING: Service Table redirection detected
origKiServiceTbl: 0x804d7000 - 0x804d7500
currKiServiceTbl: 0x804e48b0 - 0x804e4d20
pciide.sys          <f7c87000 - f7c88000>... Wrong PE image format!
Null.SYS           <f2d51000 - f2d52000>... error code = 0x490
SYSTEM INFECTION LEVEL: 1
0 - BLUE
--> 1 - GREEN
2 - YELLOW
3 - ORANGE
4 - RED
5 - DEEPRED
Nothing suspected was detected.
C:\Documents and Settings\Administrator\Desktop\hx>svv check
ntdll.dll          <77f80000 - 77ffd000>... suspected! (verdict = 5).
KERNEL32.DLL       <7c570000 - 7c623000>... suspected! (verdict = 5).
WS2_32.dll         <75030000 - 75044000>... suspected! (verdict = 5).
ADVAPI32.DLL       <7c2d0000 - 7c332000>... suspected! (verdict = 5).
SYSTEM INFECTION LEVEL: 5
0 - BLUE
1 - GREEN
2 - YELLOW
3 - ORANGE
4 - RED
--> 5 - DEEPRED
SUSPECTED modifications detected. System is probably infected!
C:\Documents and Settings\Administrator\Desktop\hx>

```

Foreground Window (C:\WINDOWS\system32\cmd.exe):

```

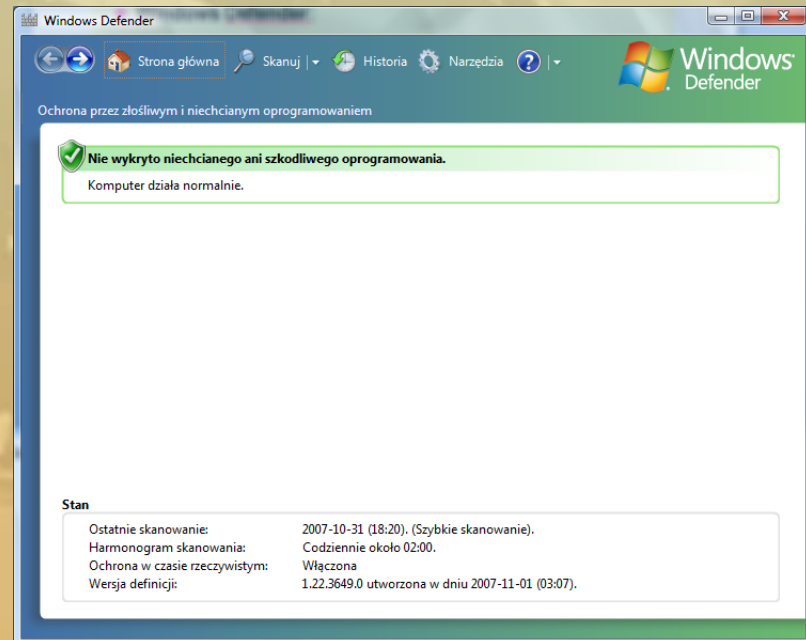
C:\WINDOWS\system32\cmd.exe
SYSTEM INFECTION LEVEL: 1
0 - BLUE
--> 1 - GREEN
2 - YELLOW
3 - ORANGE
4 - RED
5 - DEEPRED
Nothing suspected was detected.
C:\Documents and Settings\Administrator\Desktop\hx>svv check
ntdll.dll          <77f80000 - 77ffd000>... suspected! (verdict = 5).
KERNEL32.DLL       <7c570000 - 7c623000>... suspected! (verdict = 5).
WS2_32.dll         <75030000 - 75044000>... suspected! (verdict = 5).
ADVAPI32.DLL       <7c2d0000 - 7c332000>... suspected! (verdict = 5).
SYSTEM INFECTION LEVEL: 5
0 - BLUE
1 - GREEN
2 - YELLOW
3 - ORANGE
4 - RED
--> 5 - DEEPRED
SUSPECTED modifications detected. System is probably infected!
C:\Documents and Settings\Administrator\Desktop\hx>

```


Wbudowane zabezpieczenia

■ Windows Defender:

- Wykrywanie, czyszczenie i blokowanie w trybie rzeczywistym szkodliwego oprogramowania (malware, spyware, rootkits)
- Narzędzia dodatkowe!



Wbudowane zabezpieczenia

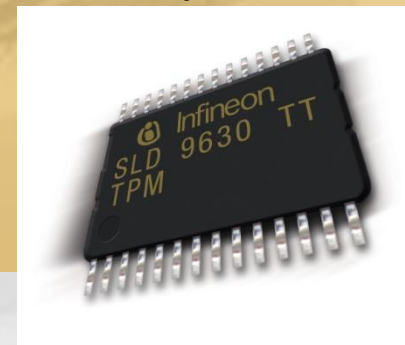
■ Internet Explorer 7:

- Tryb chroniony - IE działa bez żadnych dodatkowych uprawnień, nawet jeśli dysponuje nimi użytkownik, na przykład prawami do instalowania oprogramowania
- „Tryb tylko do odczytu”, z wyjątkiem folderu Tymczasowe pliki internetowe (dotyczy strefy zabezpieczeń Internet)
- Możliwość usuwania wszystkich danych z pamięci podręcznej przez pojedyncze kliknięcie myszą
- Filtr witryn wyłudzających informacje

Wbudowane zabezpieczenia

■ Bit Locker:

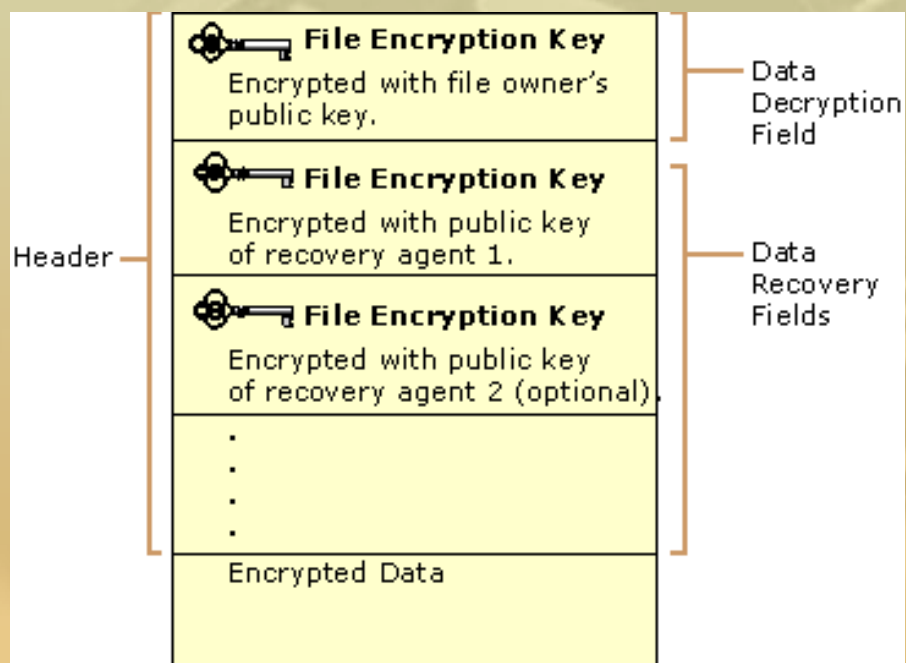
- Wykorzystuje v1.2 TPM lub pamięć USB do przechowywania klucza
- Chroni dysk systemowy przed odczytaniem gdy system jest wyłączony
 - Szyfruje cały wolumin łącznie z danymi użytkownika, plikami tymczasowymi, plikiem wymiany etc.
- Zapewnia integralność procesu uruchamiania systemu
- Upraszcza proces utylizacji dysków twardych



Wbudowane zabezpieczenia

■ System szyfrowania plików (EFS):

- Właściwość pliku lub folderu - przezroczyste dla użytkownika



Wbudowane zabezpieczenia

■ Ochrona plików systemowych:

- Kontrola procesu uruchamiania systemu obejmuje sprawdzenie sterowników, modułów jądra i HAL

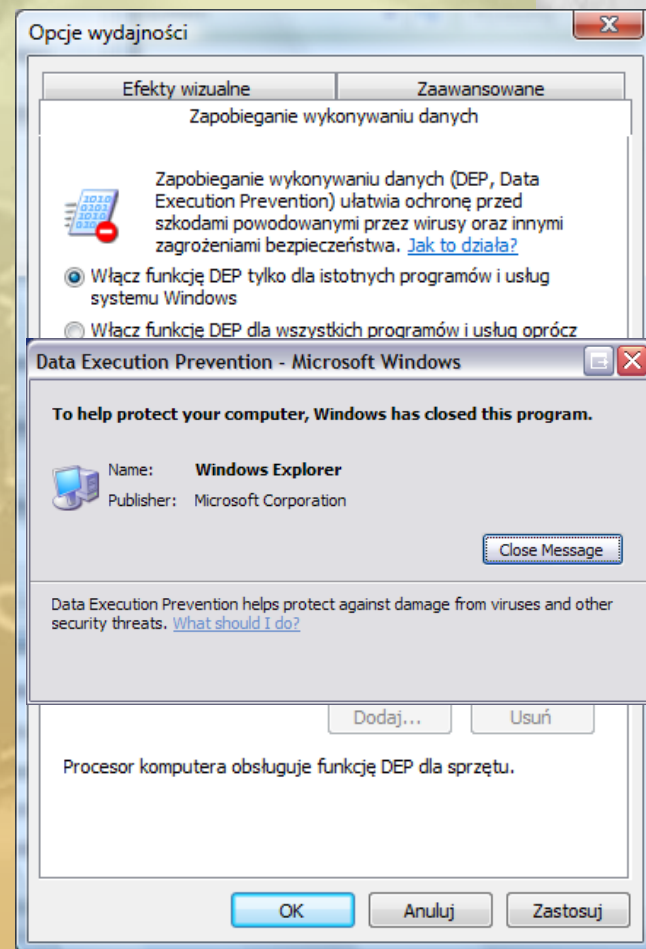
■ Zaimplementowano jako sterownik filtra systemu plików

- Sprawdza sygnatury każdej ładowanej do pamięci strony
- Sprawdza każdy obraz ładowany do procesu chronionego (Protected Process)
- Sygnatury przechowywane są w katalogu systemowym bądź w certyfikacie X.509 dołączonym do pliku

Wbudowane zabezpieczenia

■ Zapobieganie wykonywaniu danych (DEP):

- Bazuje na sprzętowych technikach oznaczania pamięci jako zawierając kod wykonywalny:
 - AMD - NX ("No Execute")
 - Intel - XD ("Execute Disable")
- W wersji 64. bitowej obligatoryjne



Wbudowane zabezpieczenia

■ Kontrola instalowanych urządzeń PnP:

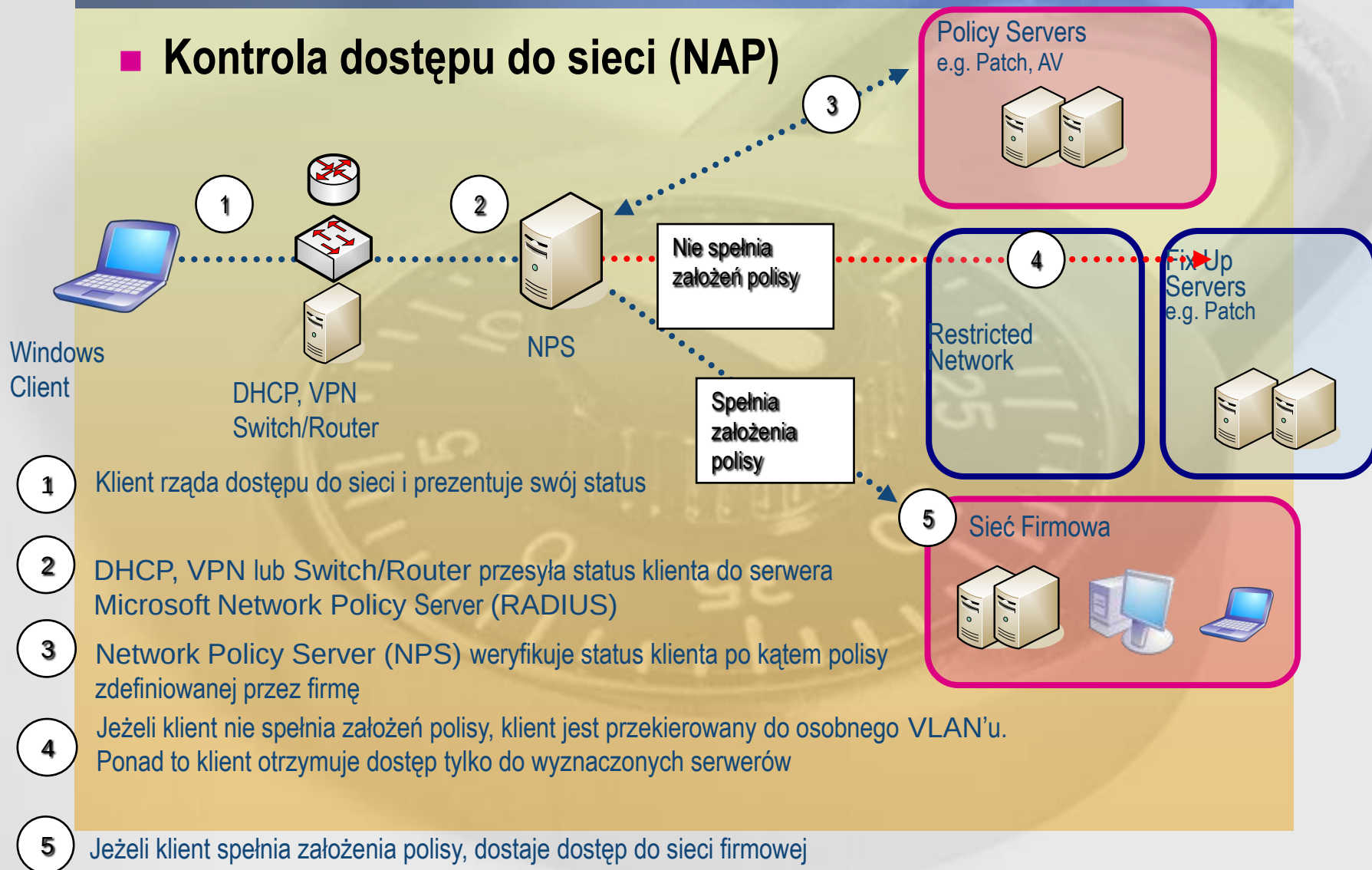
- Głównie na potrzeby wyłączania instalacji urządzeń USB, gdyż wiele korporacji obawia się wycieku własności intelektualnej
- Kontrola na podstawie klasy urządzenia

■ Zaakceptowane urządzenia mogą być wstępnie wpisane do zaufanego Magazynu sterowników (Driver Store)

- Gdy sterownik zostanie umieszczony w magazynie sterowników przez administratora, to mogą być instalowane niezależnie od uprawnień aktualnie zalogowanego użytkownika

Wbudowane zabezpieczenia

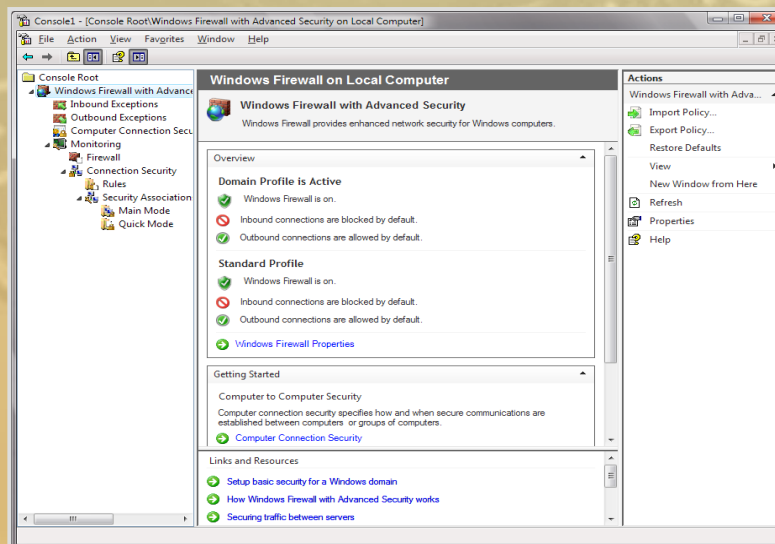
■ Kontrola dostępu do sieci (NAP)



Wbudowane zabezpieczenia

■ Zapora systemu Windows:

- Komunikacja wychodząca i przychodząca
- Zintegrowania z IPSec
- Uwzględnia uwierzytelnianie i autoryzację



Kontrola konta użytkownika

■ Implementacja modelu Bella-LaPaduli:

- Podmiot może zapisać dane w obiekcie, jeżeli poziom uprawnień tego podmiotu jest zdominowany przez poziom zabezpieczeń obiektu
- Każdy proces (program lub usługa systemowa) działa na określonym poziomie zaufania, a każdy obiekt (na przykład plik) jest sklasyfikowany na pewnym poziomie zaufania. Ponieważ obowiązuje zasada zezwalająca jedynie na modyfikowanie zdominowanych obiektów, proces działający na niższym poziomie zaufania, nawet jeżeli został uruchomiony przez administratora, nie zmodyfikuje zaufanych (czyli systemowych) obiektów
- Utworzony przez proces obiekt dziedziczy jego poziom zaufania

Kontrola konta użytkownika

- **Ułatwia realizację zasady najmniejszych uprawnień na dwa różne sposoby:**
 - Wszyscy użytkownicy są standardowymi użytkownikami
 - Stare, czy bardziej „zachłanne” aplikacje są wirtualizowane
- **Każda potrzeba prawdziwego wykorzystania uprawnień administratorskich wymaga:**
 - Wskazania użytkownika, który te uprawnienia ma, lub
 - Potwierdzenia chęci wykonania danej operacji
- **Domyślnie programy działają z ograniczonymi uprawnieniami**

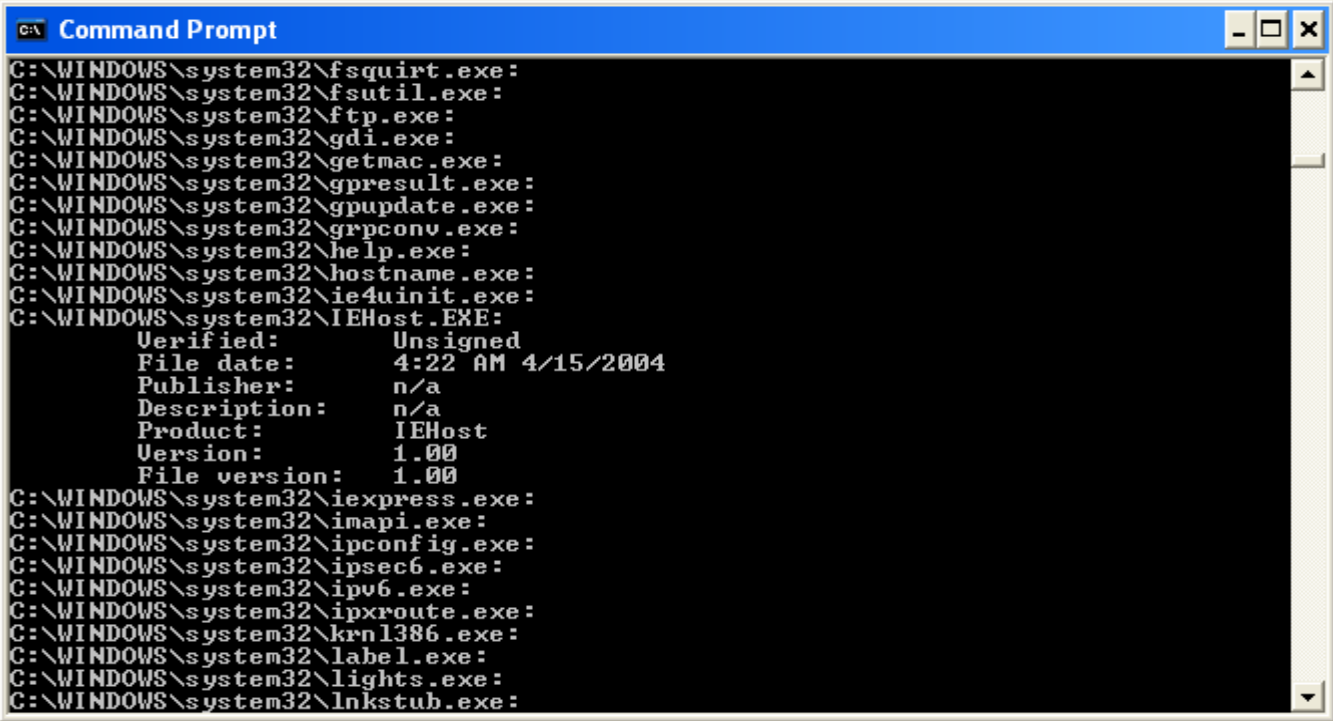
Narzędzia dodatkowe

- **Sigcheck: dostępny na witrynie**
<http://www.microsoft.com/technet/sysinternals>
- **Autoruns: dostępny na witrynie**
<http://www.microsoft.com/technet/sysinternals>
- **Process Explorer: dostępny na witrynie**
<http://www.microsoft.com/technet/sysinternals>
- **Dostęp offline: Konsola odzyskiwania, Windows PE, ERD Commander, BartPE**

Narzędzia dodatkowe - Sigcheck

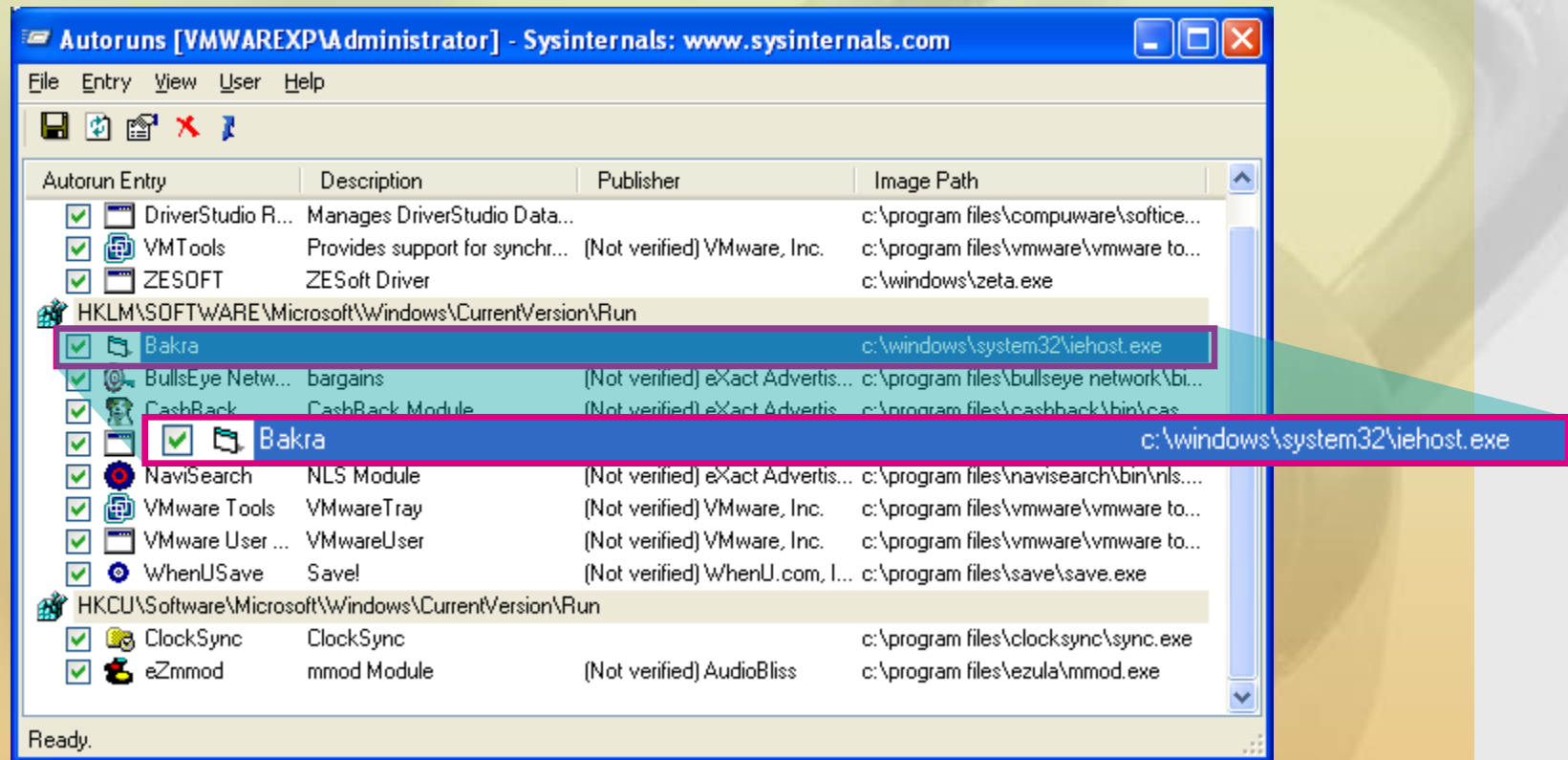
- Wyświetla informacje o niepodpisanych cyfrowo plikach:

sigcheck -e -u -s c:



```
Command Prompt
C:\WINDOWS\system32\fsquirt.exe:
C:\WINDOWS\system32\fsutil.exe:
C:\WINDOWS\system32\ftp.exe:
C:\WINDOWS\system32\gdi.exe:
C:\WINDOWS\system32\getmac.exe:
C:\WINDOWS\system32\gpresult.exe:
C:\WINDOWS\system32\gpupdate.exe:
C:\WINDOWS\system32\grpconv.exe:
C:\WINDOWS\system32\help.exe:
C:\WINDOWS\system32\hostname.exe:
C:\WINDOWS\system32\ie4uinit.exe:
C:\WINDOWS\system32\IEHost.EXE:
    Verified:      Unsigned
    File date:     4:22 AM 4/15/2004
    Publisher:     n/a
    Description:   n/a
    Product:       IEHost
    Version:       1.00
    File version:  1.00
C:\WINDOWS\system32\iexpress.exe:
C:\WINDOWS\system32\imapi.exe:
C:\WINDOWS\system32\ipconfig.exe:
C:\WINDOWS\system32\ipsec6.exe:
C:\WINDOWS\system32\ipv6.exe:
C:\WINDOWS\system32\ipxroute.exe:
C:\WINDOWS\system32\krnl386.exe:
C:\WINDOWS\system32\label.exe:
C:\WINDOWS\system32\lights.exe:
C:\WINDOWS\system32\lnkstub.exe:
```

Narzędzia dodatkowe - Autoruns



Narzędzia dodatkowe - Process Explorer

