System operacyjny

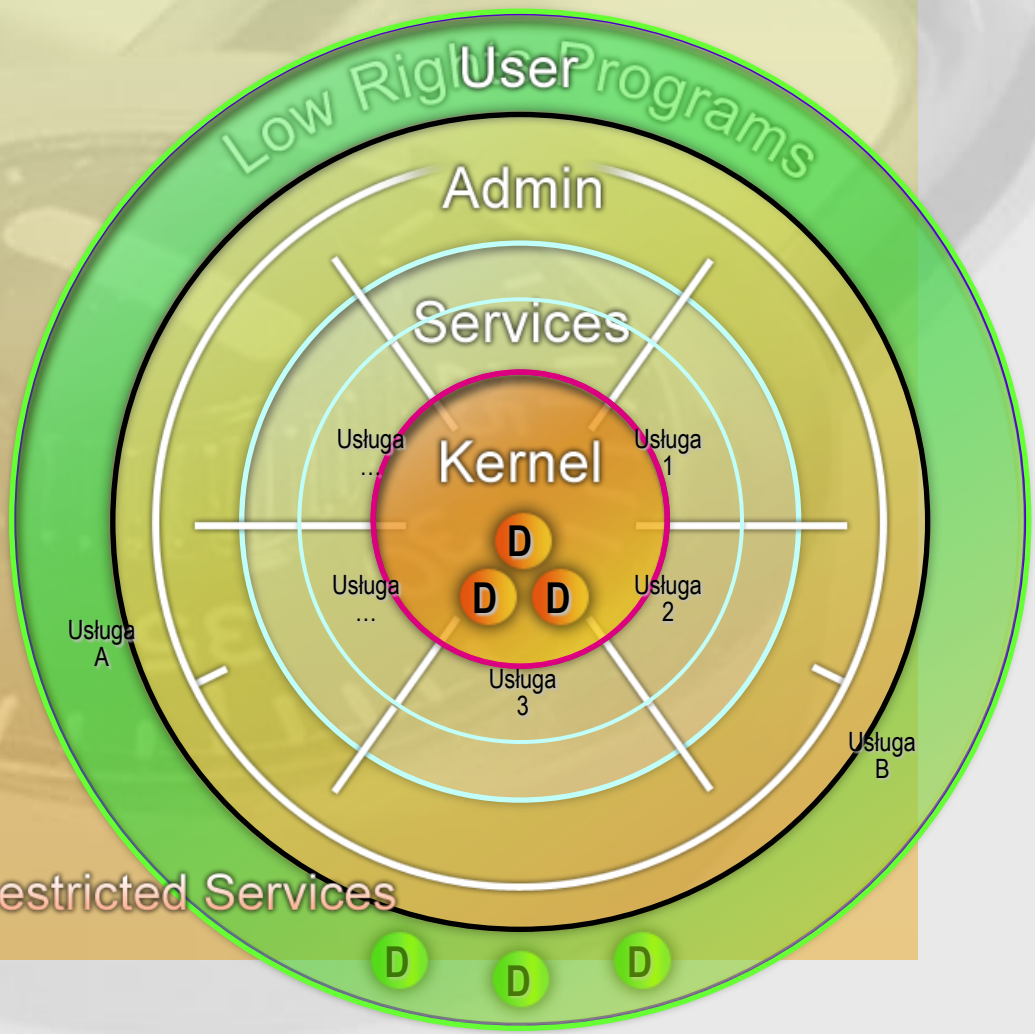
Marcin Szeliga
marcin@wss.pl

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 trubu 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

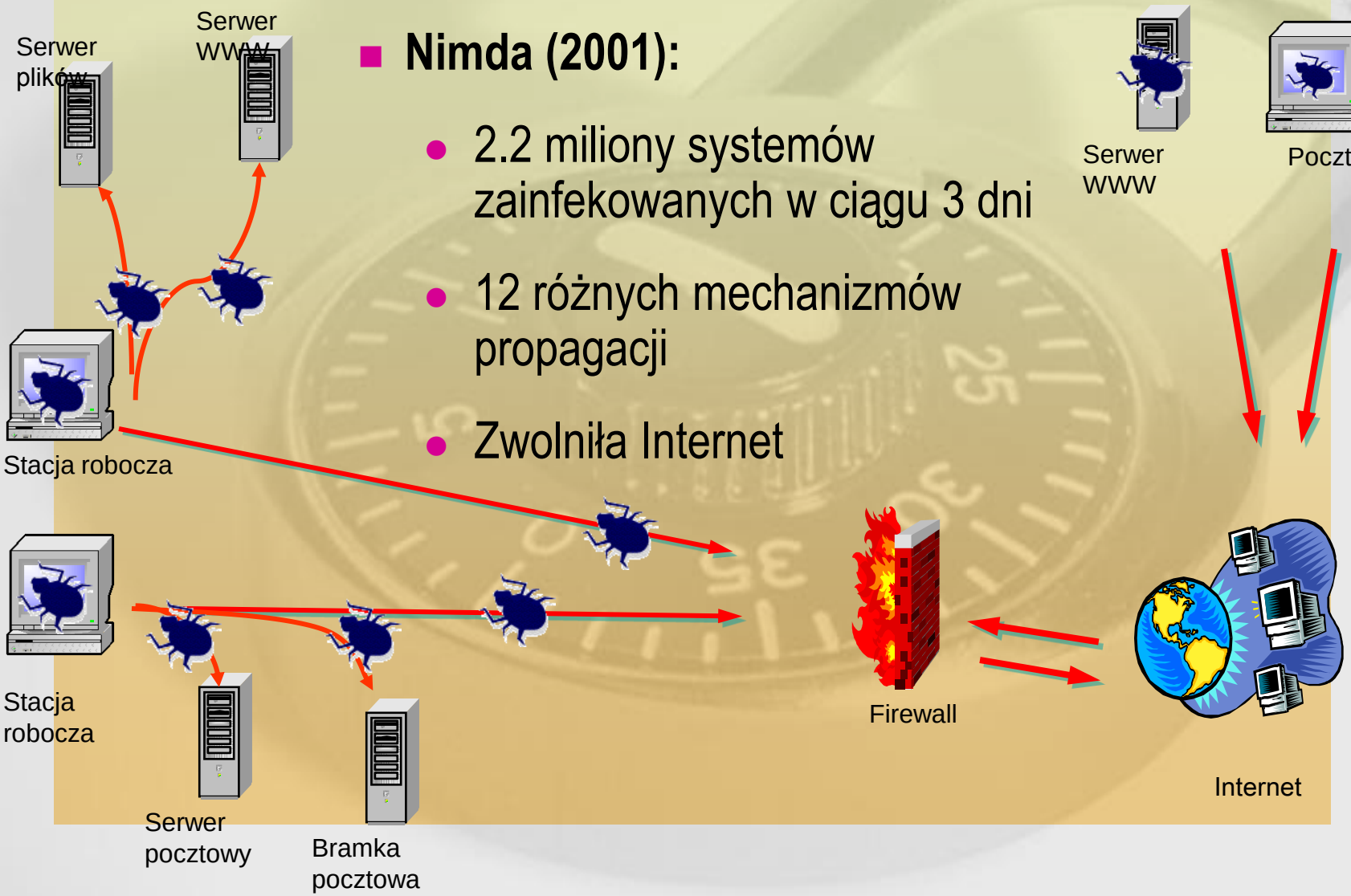
Aplikacja 1
Aplikacja 2
Aplikacja 3

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

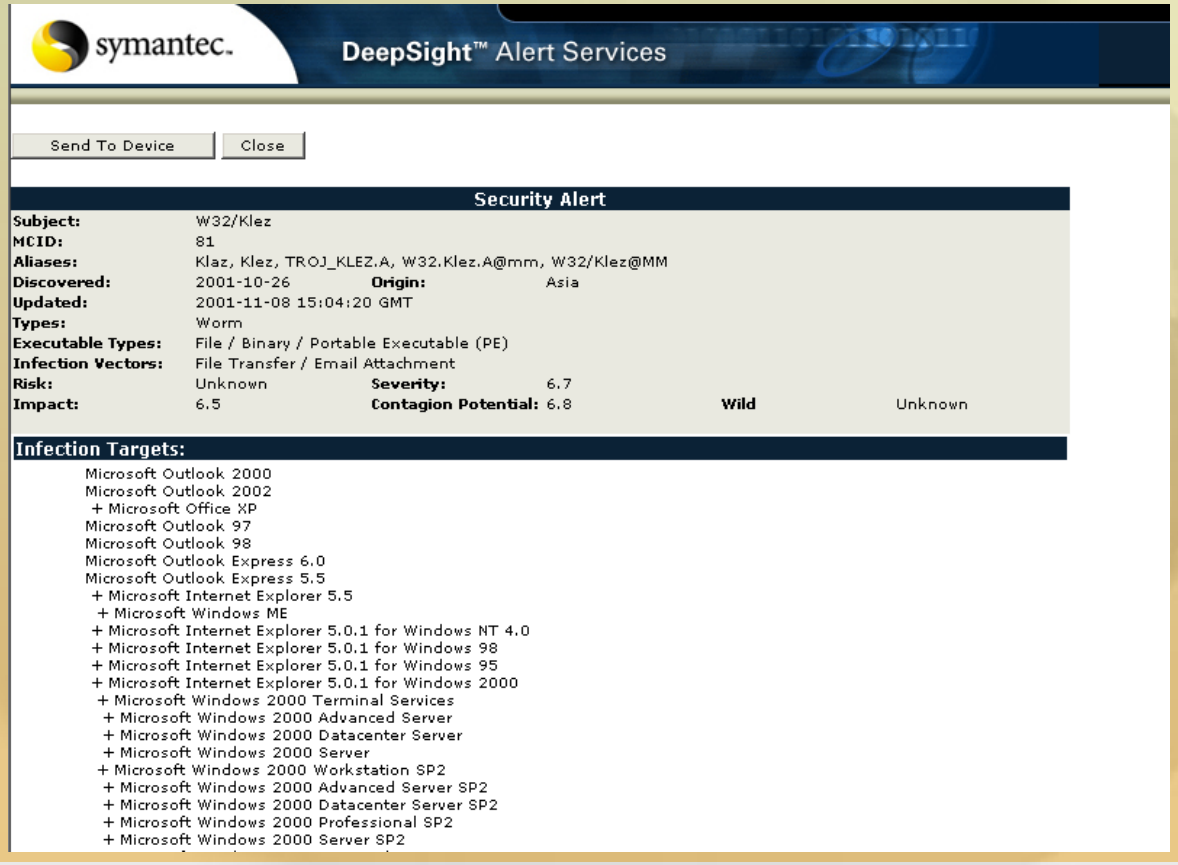
Zagrożenia - wirusy

- **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



symantec. DeepSight™ Alert Services

Send To Device | Close

Security Alert

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

Infection 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

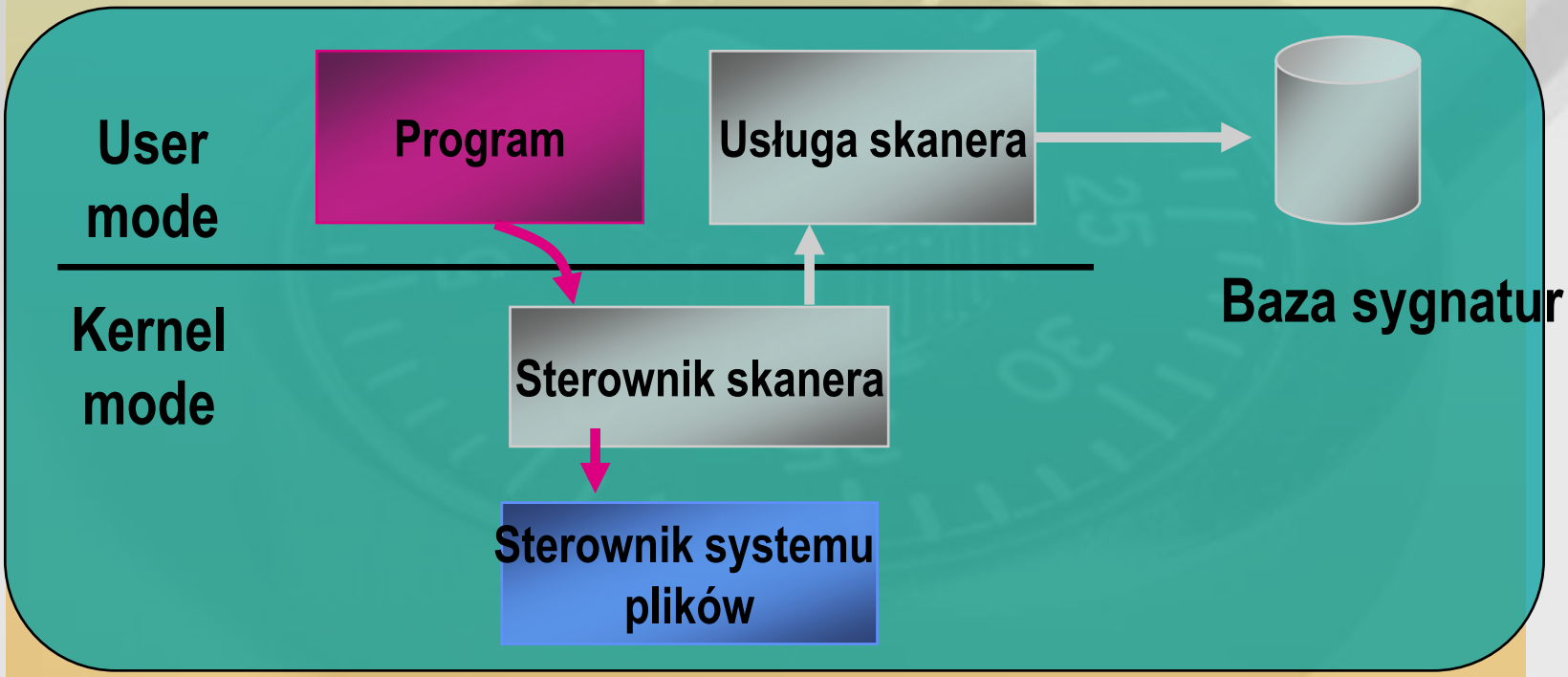
- **SLAMMER (2003) potrzebował tylko 10 minut**
  - Ponad 90% podatnych na atak serwerów SQL zostało zainfekowane w ciągu 10 minut.
  - Podwojenie liczby zainfekowanych maszyn następowało co 8.5 sekundy (w przypadku robaka CodeRed było to 37 minut)
  - Z powodu zalania sieci m.in. odwołano loty i wyłączono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

Zagrożenia - Wirusy

- **ZOTOB (2005):**
  - Został napisany na zamówienie przez Turka i Marokańczyka
  - Sparaliżował CNN live
  - A następnie wybrane firmy, głownie banki

Zagrożenia - wirusy

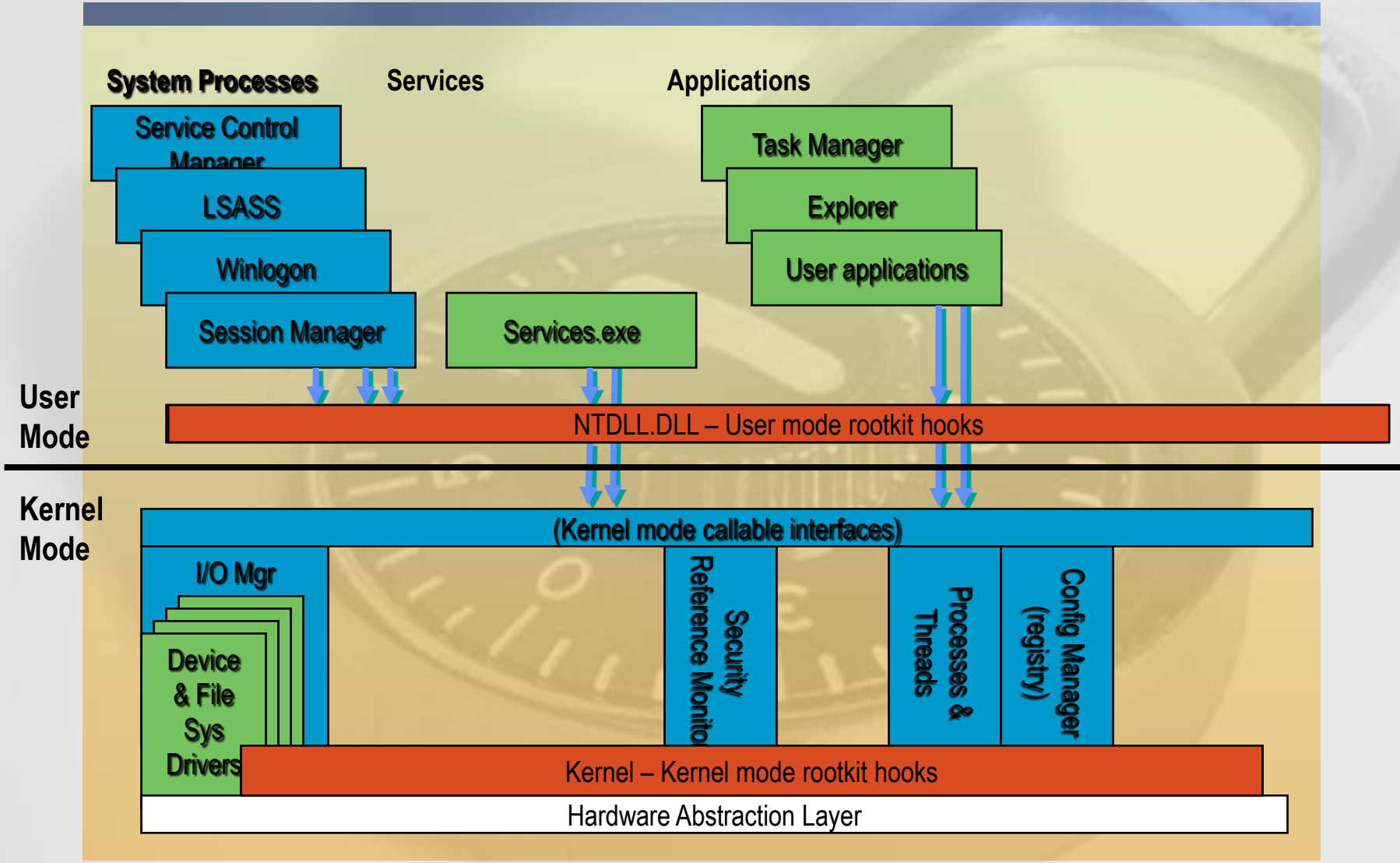
- Programy antywirusowe bazują na sygnaturach
- Przechwytują operacje I/O



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



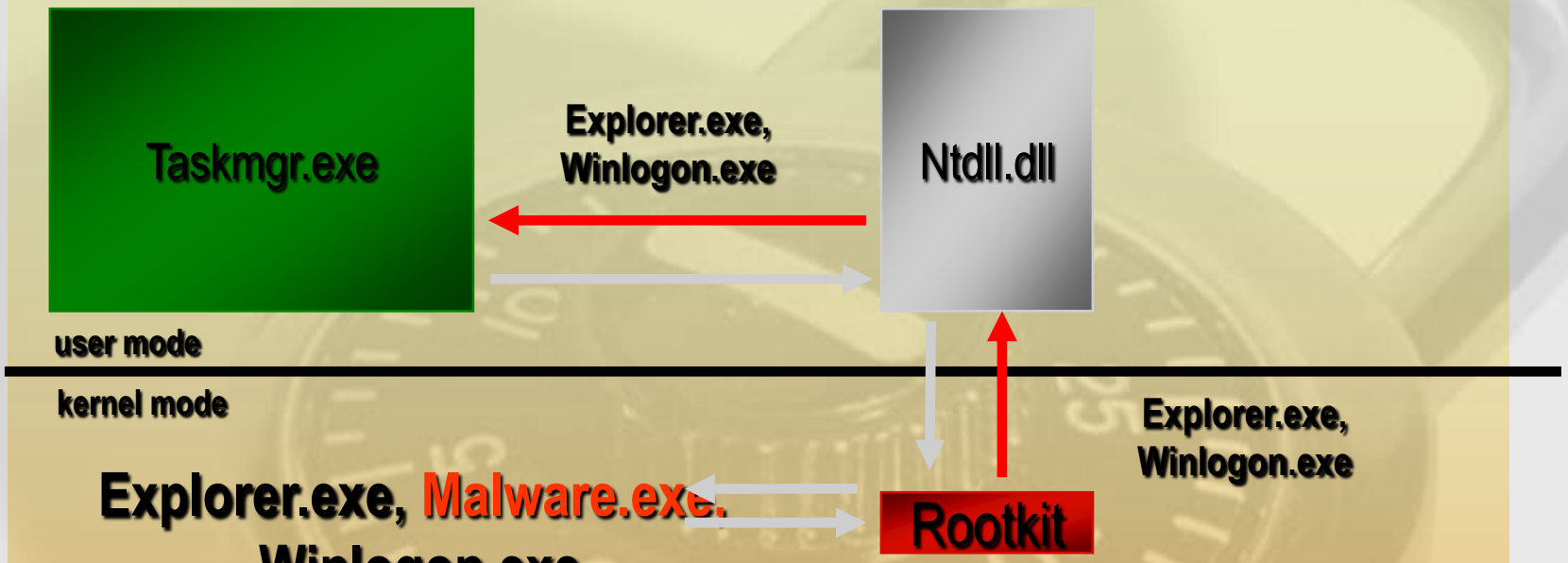
Zagrożenia – Rootkity (API użytkownika)

- 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



- Zalety: Trudne do wykrycia, skuteczne
- Wady: Wymagają uprawnień administratora, trudne do napisania
- Przykład: NT Rootkit

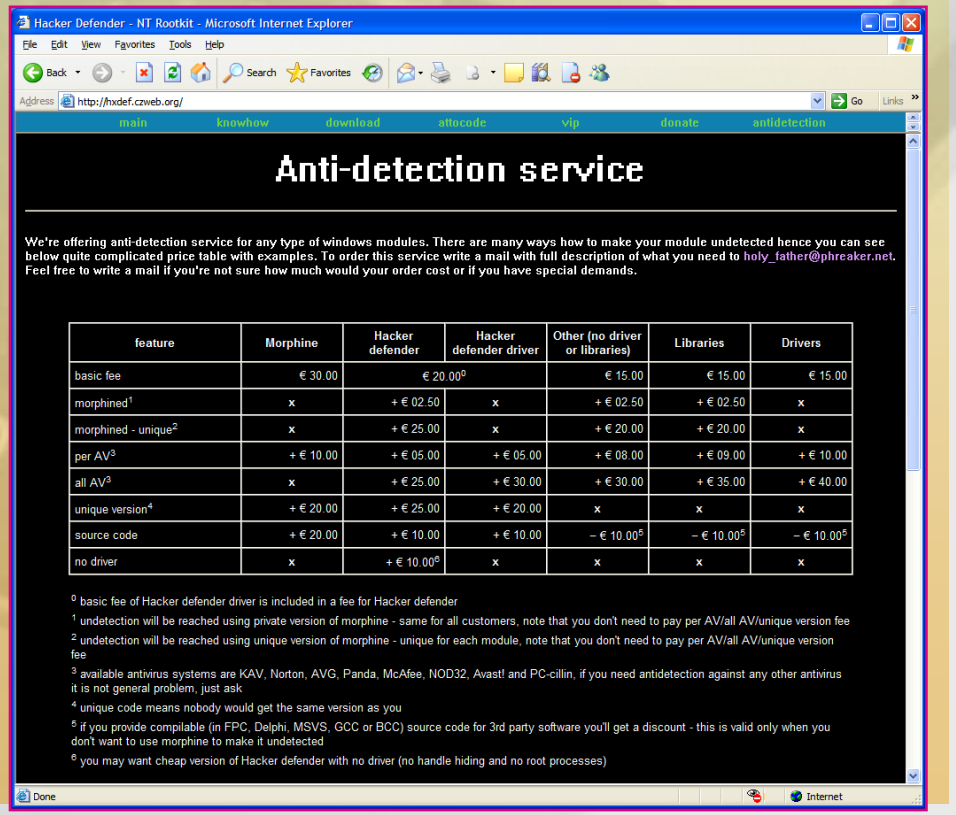
Zagrożenia – Rootkity (modyfikacja jądra systemu)

- **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



Hacker Defender - NT Rootkit - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://hxdef.czweb.org/ Go Links

main knowhow download attocode vip donate antidetection

Anti-detection service

We're offering anti-detection service for any type of windows modules. There are many ways how to make your module undetected hence you can see below quite complicated price table with examples. To order this service write a mail with full description of what you need to holy_father@phreaker.net. Feel free to write a mail if you're not sure how much would your order cost or if you have special demands.

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

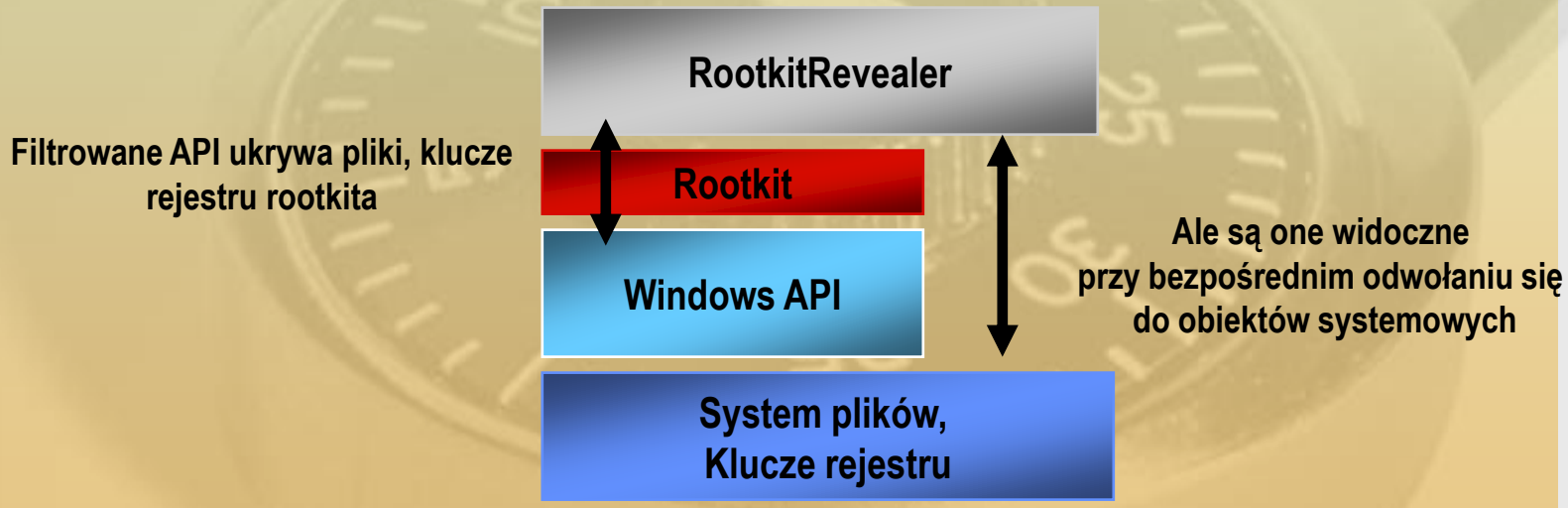
[5] if you provide compilable (in FPC, Delphi, MSVS, GCC or BCC) source code for 3rd party software you'll get a discount - this is valid only when you don't want to use morphine to make it undetected

[6] you may want cheap version of Hacker defender with no driver (no handle hiding and no root processes)

Done Internet

Zagrożenia - Rootkity

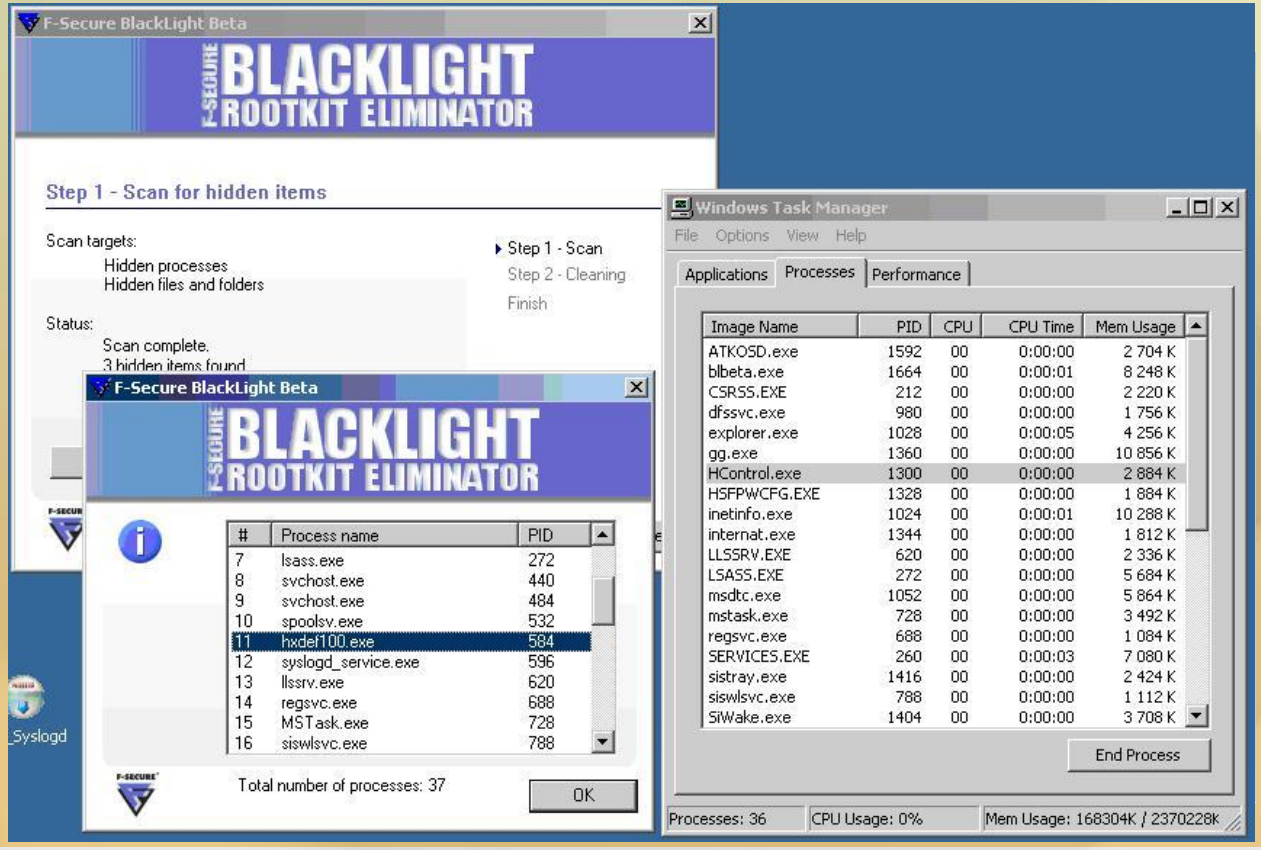
- **O wiele łatwiej jest zapobiegać ich instalacji niż je wykryć**
  - Nie filtrują całego API, mają zauważalne efekty uboczne i nie działają, gdy system jest wyłączony



- **Automatyczne usunięcie jest z reguły niemożliwe**

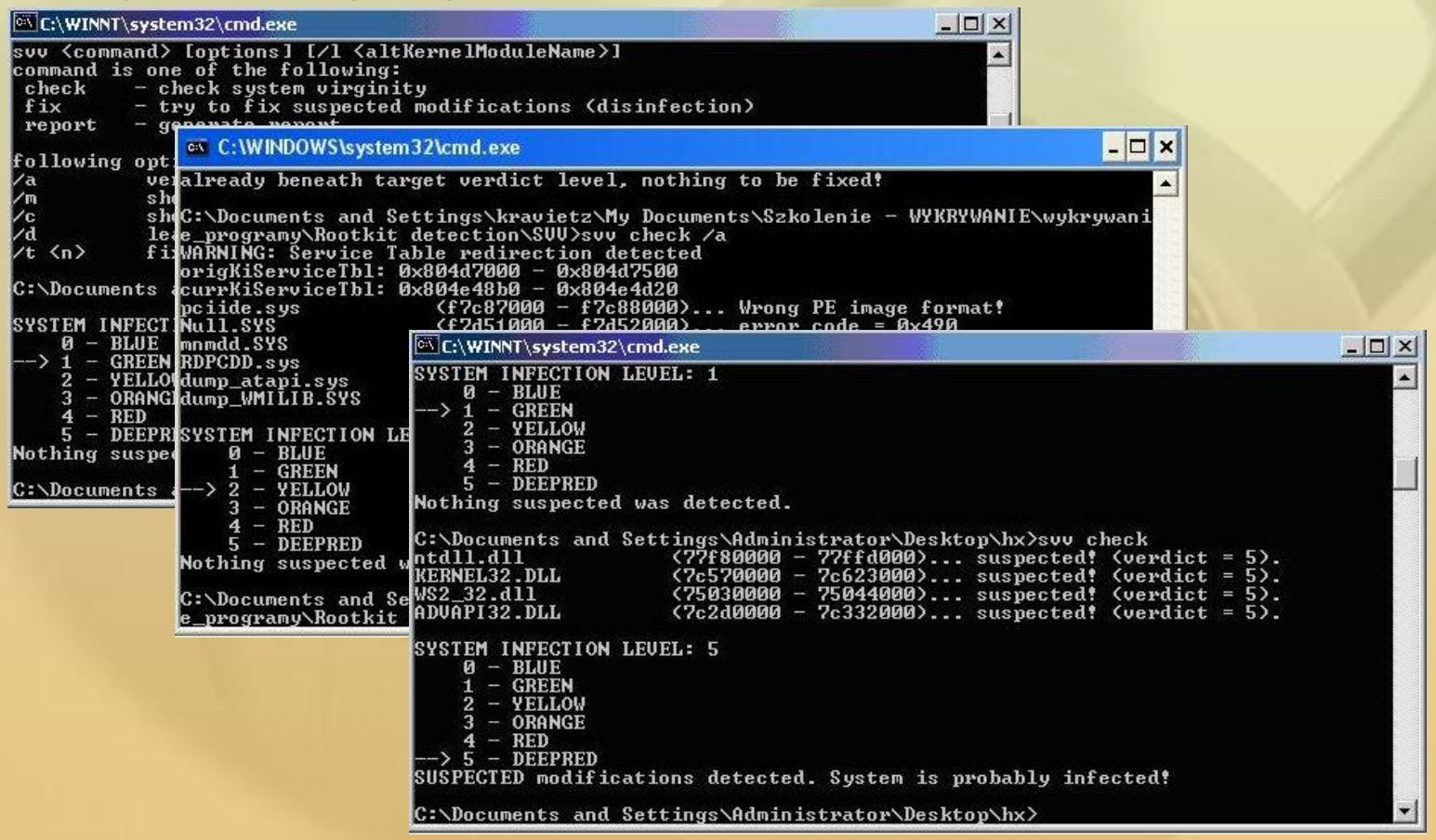
Zagrożenia - Rootkity

- Rootkir Revealer
- Black Light



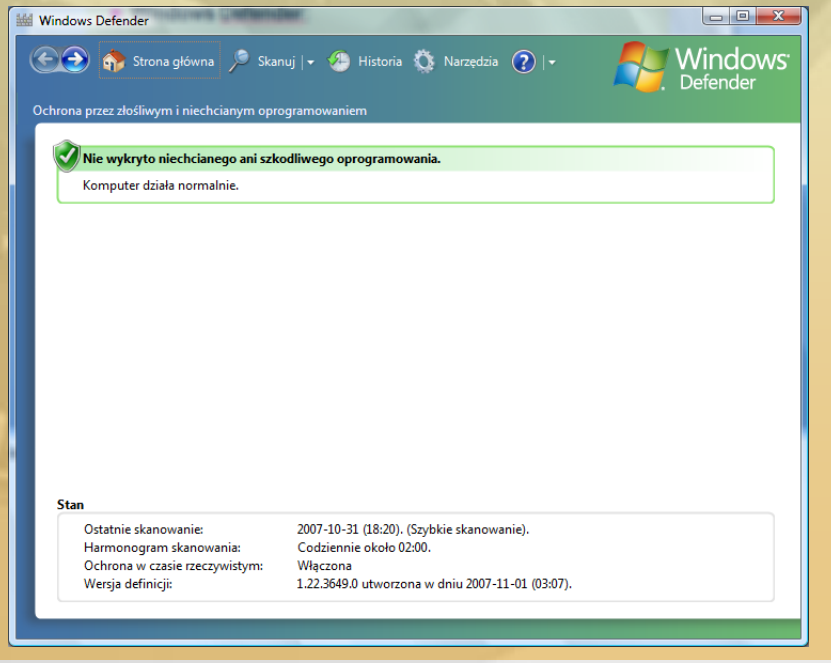
Zagrożenia - Rootkity

- System Virginity Verifier



Wbudowane zabezpieczenia

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

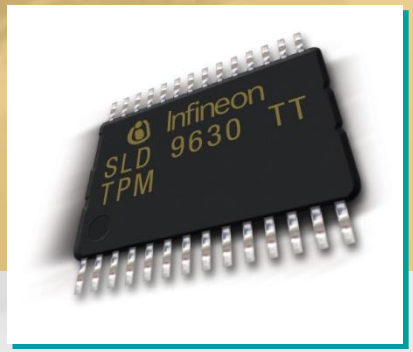


Wbudowane zabezpieczenia

- **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

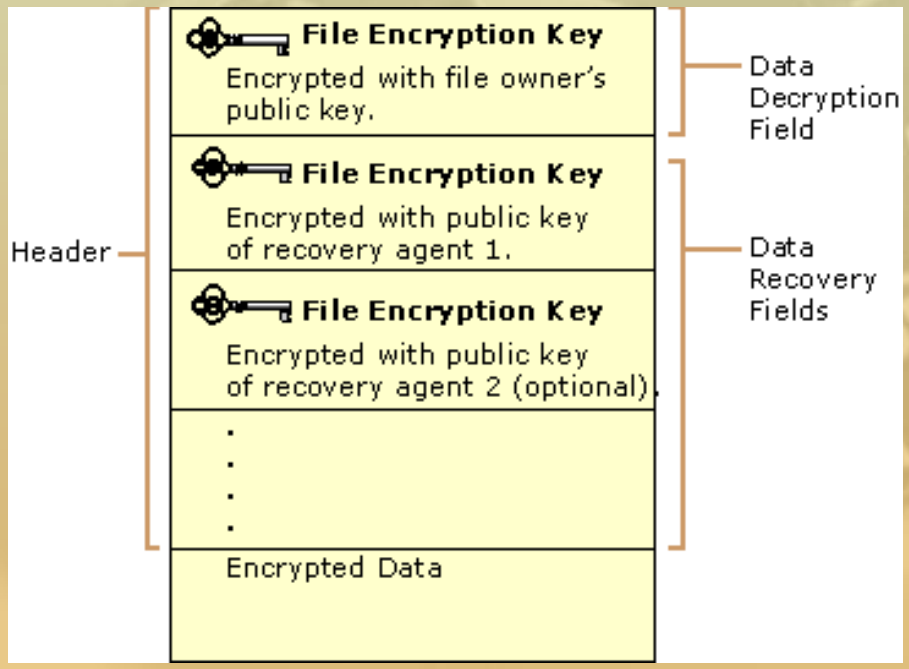
Wbudowane zabezpieczenia

- **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

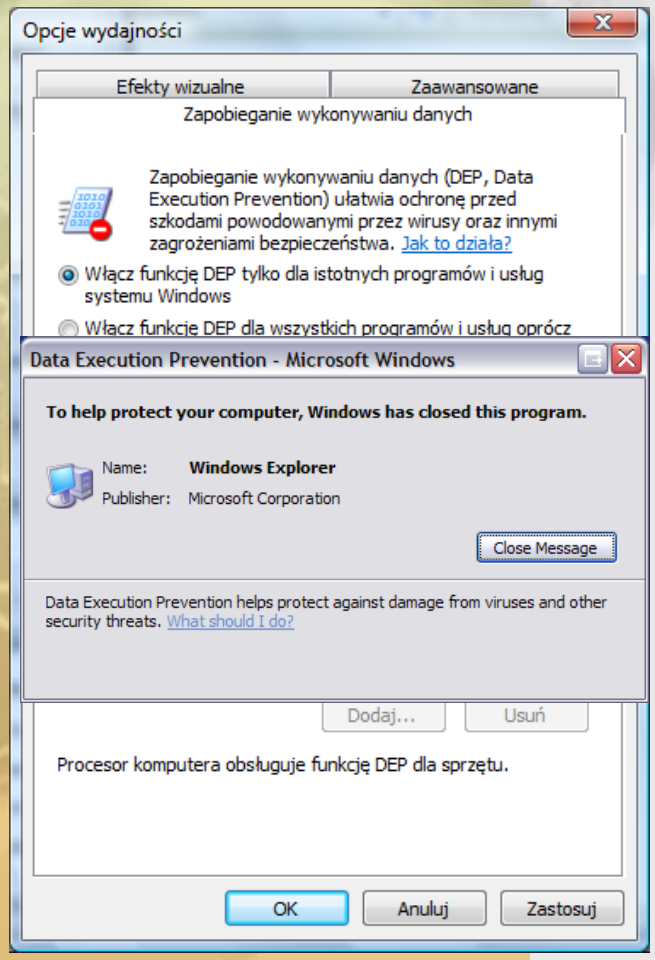


Wbudowane zabezpieczenia

- **Ochrona plików systemowych:**
  - Kontrola procesu uruchamiania systemu obejmuje sprawdzenie sterowników, modułów jądra i HAL
- **Zaimplementowano jako sterownik filtru 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

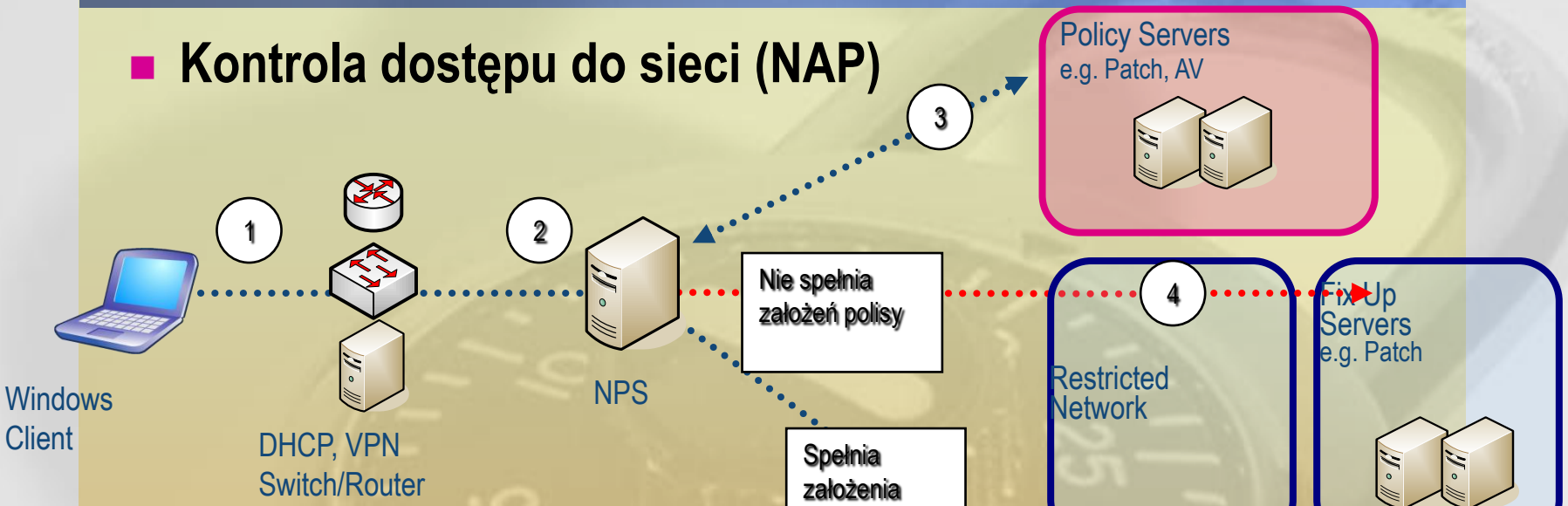


Wbudowane zabezpieczenia

- **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 użytkownik

Wbudowane zabezpieczenia

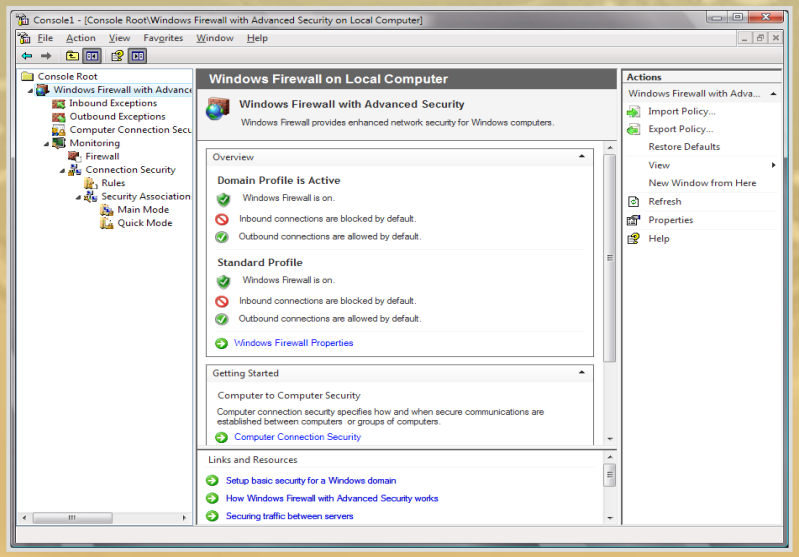
Kontrola dostępu do sieci (NAP)



1. Klient rząda dostępu do sieci i prezentuje swój status
2. DHCP, VPN lub Switch/Router przesyła status klienta do serwera Microsoft Network Policy Server (RADIUS)
3. Network Policy Server (NPS) weryfikuje status klienta po kątem polisy zdefiniowanej przez firmę
4. Jeżeli klient nie spełnia założeń polisy, klient jest przekierowany do osobnego VLAN'u. Ponad to klient otrzymuje dostęp tylko do wyznaczonych serwerów
5. Jeżeli klient spełnia założenia polisy, dostaje dostęp do sieci firmowej

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**

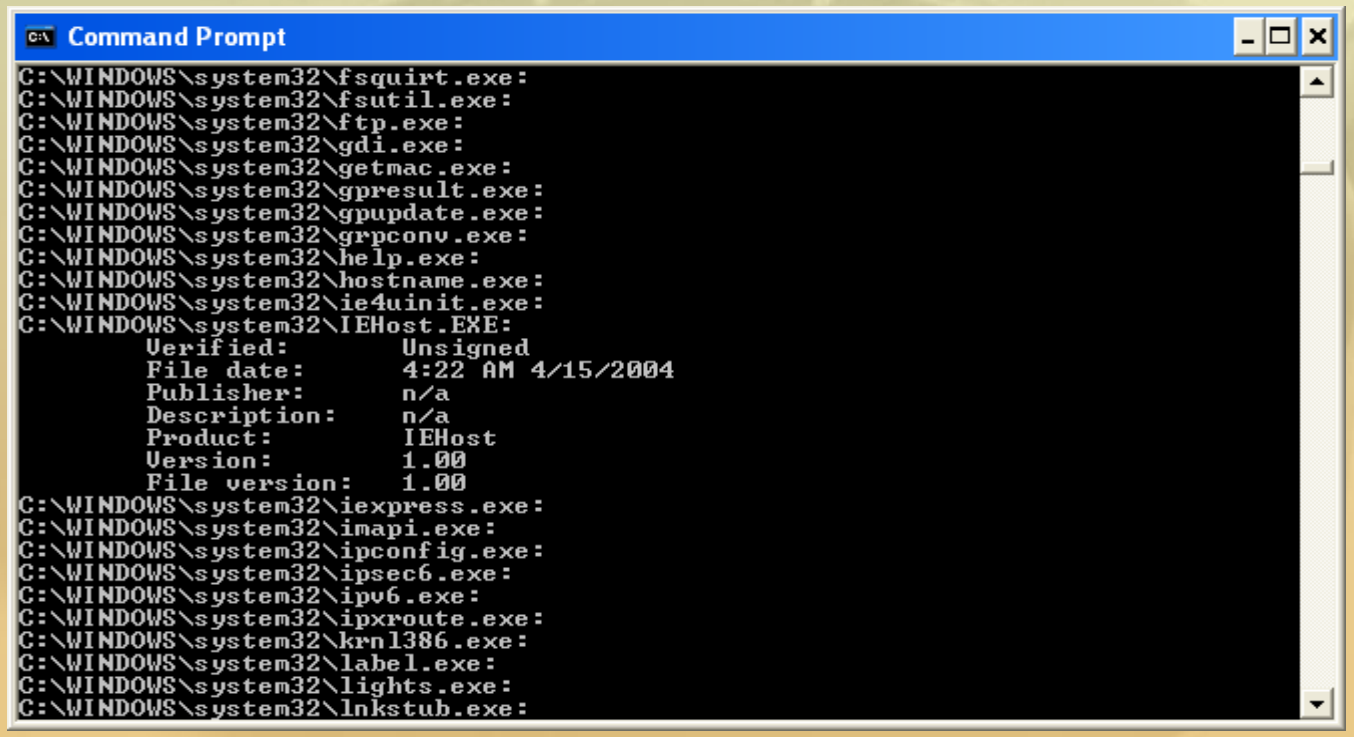
Narzędzia dodatkowe

- 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

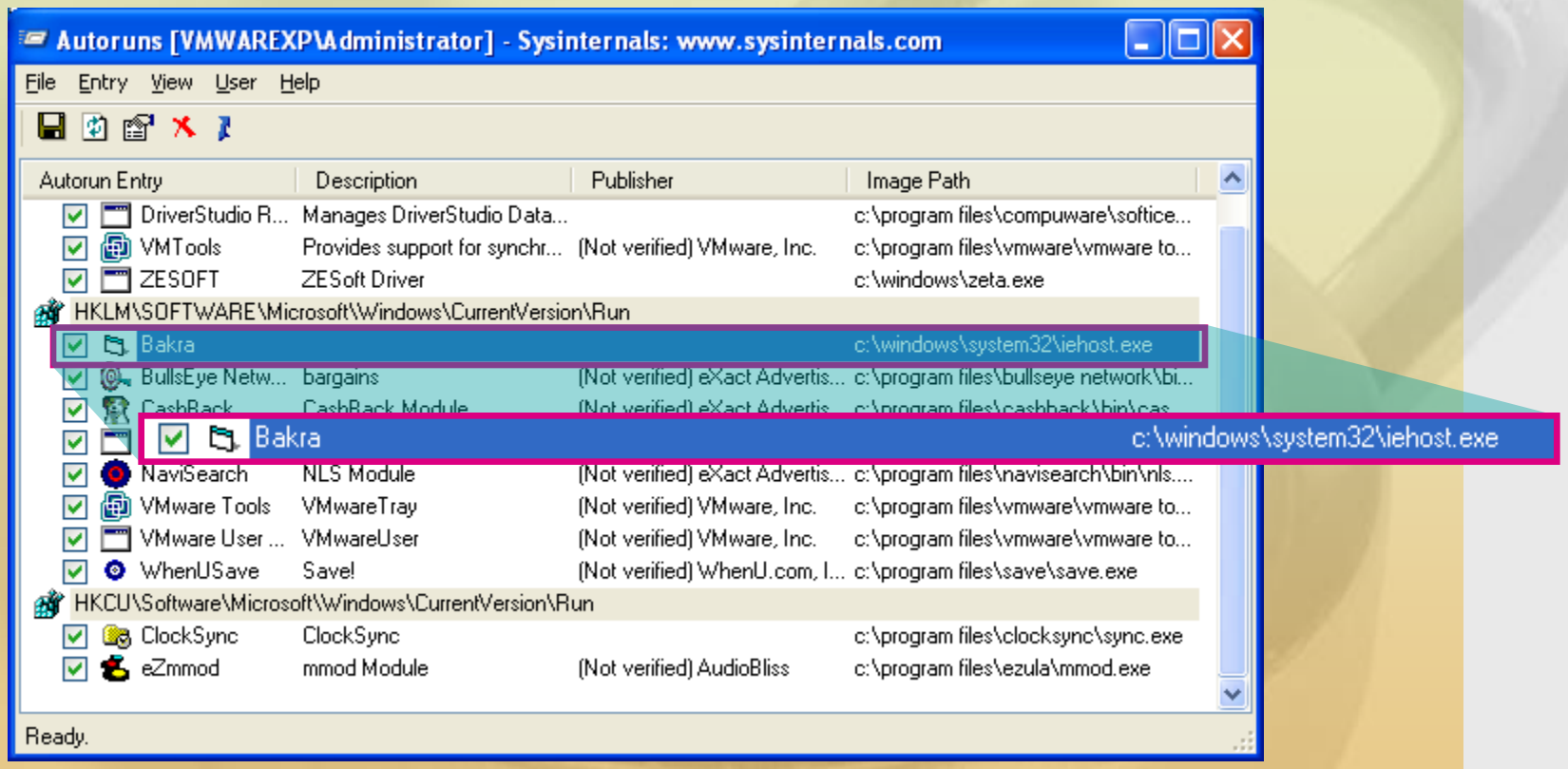
Narzędzia dodatkowe - Sigcheck

- Wyświetla informacje o niepodpisanych cyfrowo plikach:

```
sigcheck -e -u -s c:\
```



Narzędzia dodatkowe - Autoruns



Narzędzia dodatkowe - Process Explorer