Robaki sieciowe

+ systemy IDS/IPS

Robak komputerowy

(ang. *computer worm*)

- samoreplikujący się program komputerowy, podobny do wirusa komputerowego, ale w przeciwieństwie do niego nie potrzebujący nosiciela
- rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym oraz naiwności użytkownika
- może niszczyć pliki, rozsyłać spam, pełnić funkcję backdoor'a lub konia trojańskiego
- kiedyś tworzone dla idei – obecnie dla $$$
- 1978 rok – dwóch badaczy z Xerox PARC napisało pierwszy program, który można nazwać robakiem

Te paskudne robale …

- Christmas Tree Worm (grudzień 1987)
- Morris (listopad 1988)
- …
- Code Red (lipiec 2001)
- SQL Slammer (styczeń 2003)
- Blaster (sierpień 2003)
- MyDoom (luty 2004)
- Sasser (kwiecień 2004)
- Zotob (sierpień 2005)
- + wiele innych

Typy robaków :

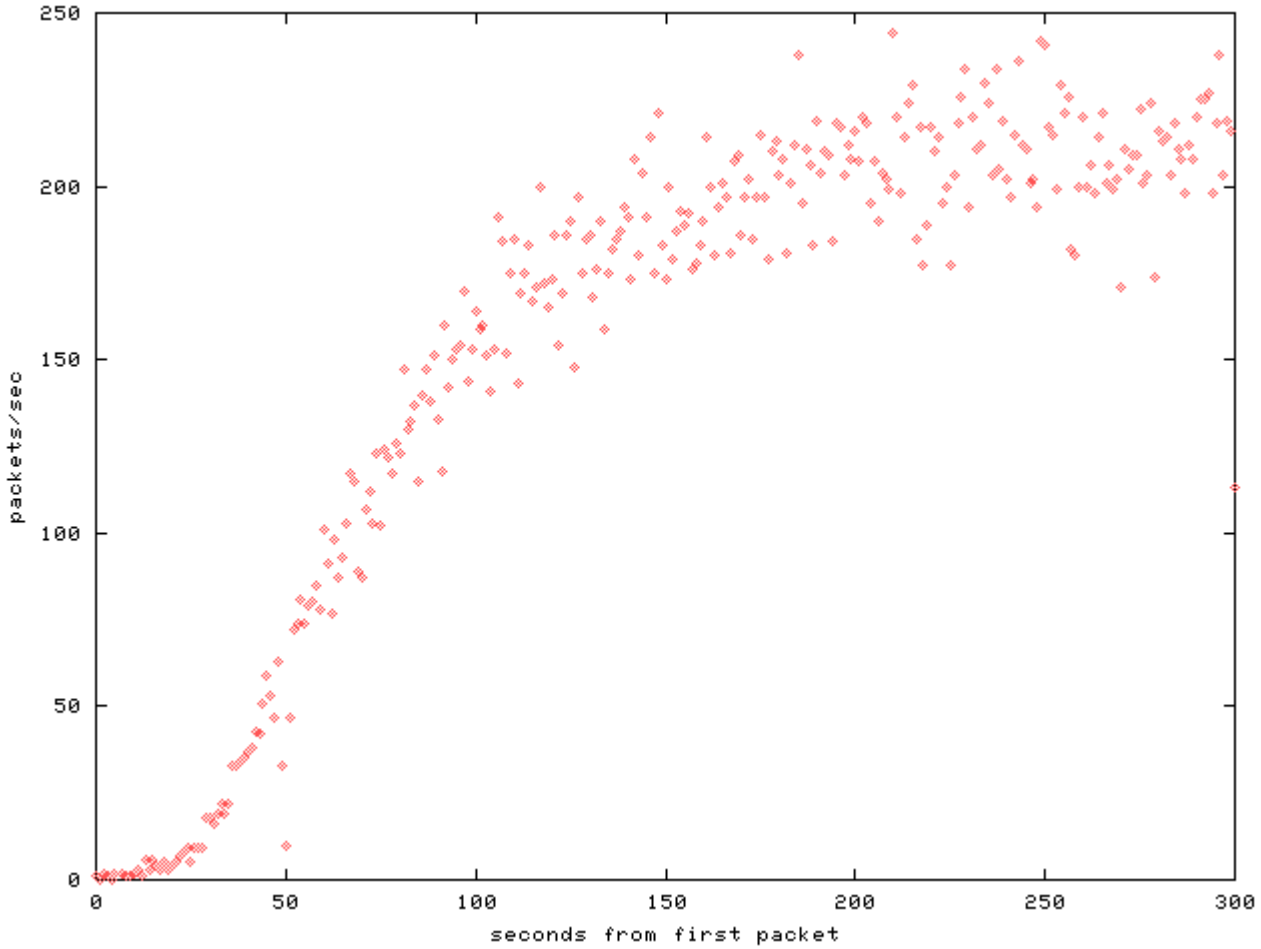
- Email worms
- Instant messaging worms
- IRC worms
- File-sharing network worms
- Internet worms

SQL Slammer

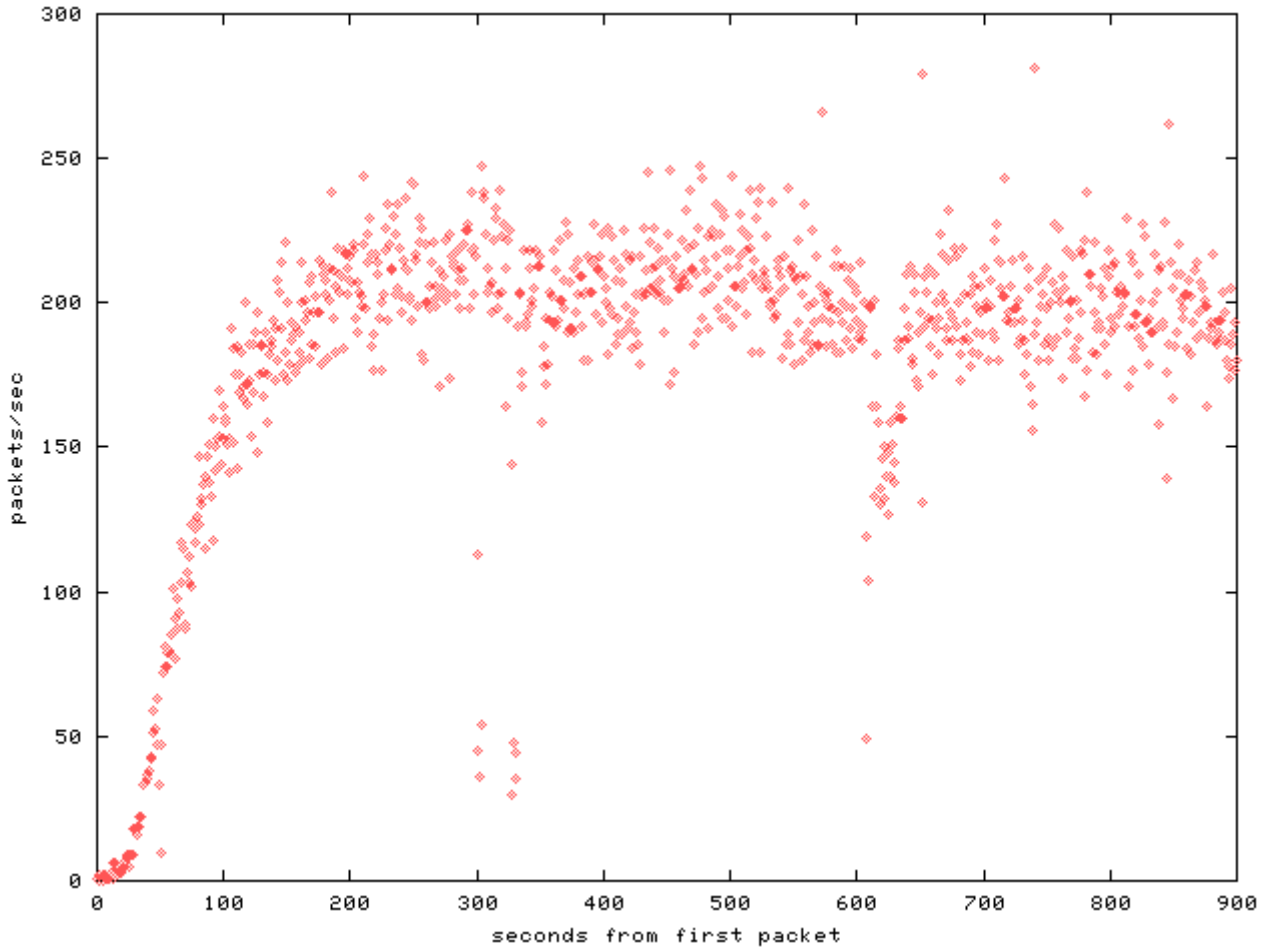
(styczeń 2003 – 376 bajtów kodu)

- zainfekował serwery Microsoft SQL na całym świecie
- tempo podwajania się zainfekowanych komputerów : osiem i pół sekundy (75000 ofiar przez pierwsze 10 minut działania!)
- wykorzystanie pakietów UDP zamiast TCP pozwoliło na generowanie gigantycznego ruchu w sieci, rzędu gigabajtów na sekundę
- główne straty wynikały z gigantycznego ruchu sieciowego a nie przejęcia serwerów MS SQL - straty poniosły zupełnie inne, nie zainfekowane serwery
- trudność w przeciwdziałaniu ataków – administratorzy zainfekowanych serwerów niespecjalnie przejmowali się infekcją, Microsoft załatał dziurę tylko tymczasowo

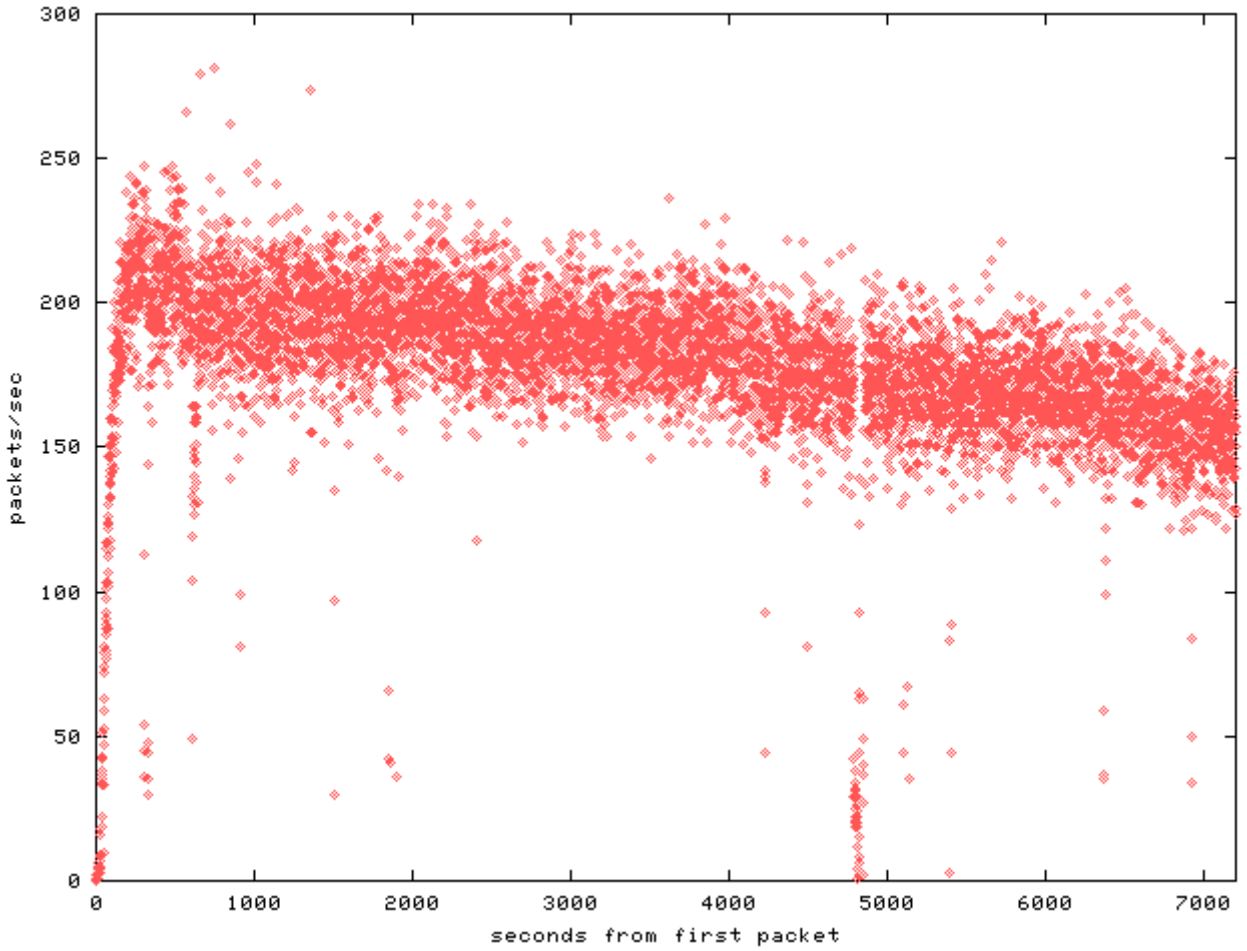
SQL Slammer


250
200
150
100
50
0
packets/sec
0
50
100
150
200
250
300
seconds from first packet

SQL Slammer


300
250
200
150
100
50
0
packets/sec
0
100
200
300
400
500
600
700
800
900
seconds from first packet

SQL Slammer

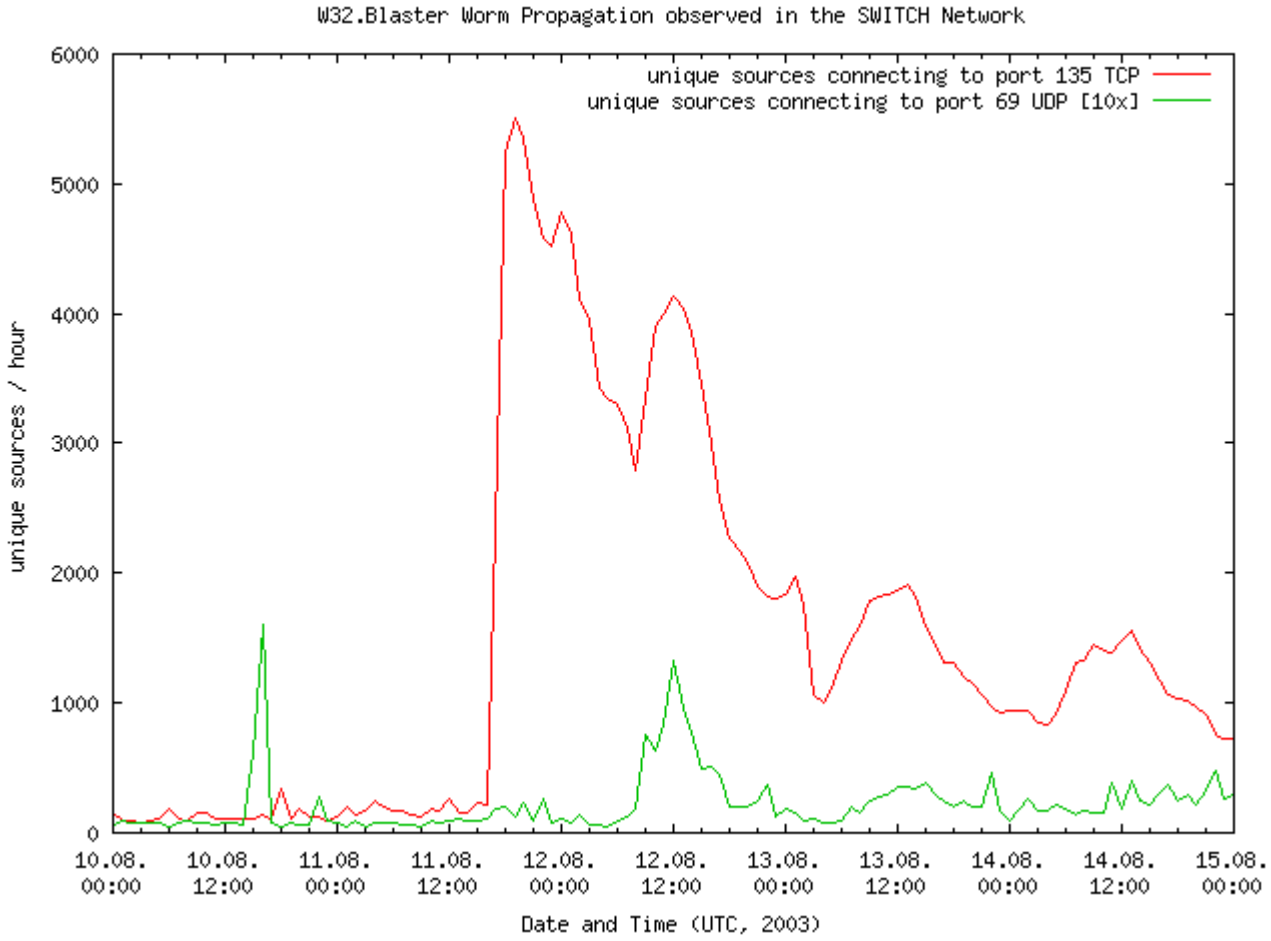

300
250
200
150
100
50
0
packets/sec
0
1000
2000
3000
4000
5000
6000
7000
seconds from first packet

Blaster

(inne nazwy : Lovsan, Lovesan)

- pojawił się 11 sierpnia 2003
- atakował poprzez port 135 (TCP)
- rozprzestrzeniał się na komputerach z zainstalowanym systemem operacyjnym Windows 2000 lub Windows XP.
- Atak typu (D)DoS ((**D**istributed) **D**enial **o**f **S**ervice attack)
- u zainfekowanego robak powodował restart systemu po minucie od połączenia z internetem
- 15 sierpnia robak miał wywołać atak typu ‘SYN flood’ na stronę z uaktualnieniami systemu Windows – atak nie wywołał większych szkód gdyż atakował stronę windowsupdate.com zamiast windowsupdate.microsoft.com (ta pierwsza to tylko przekierowanie)

Blaster

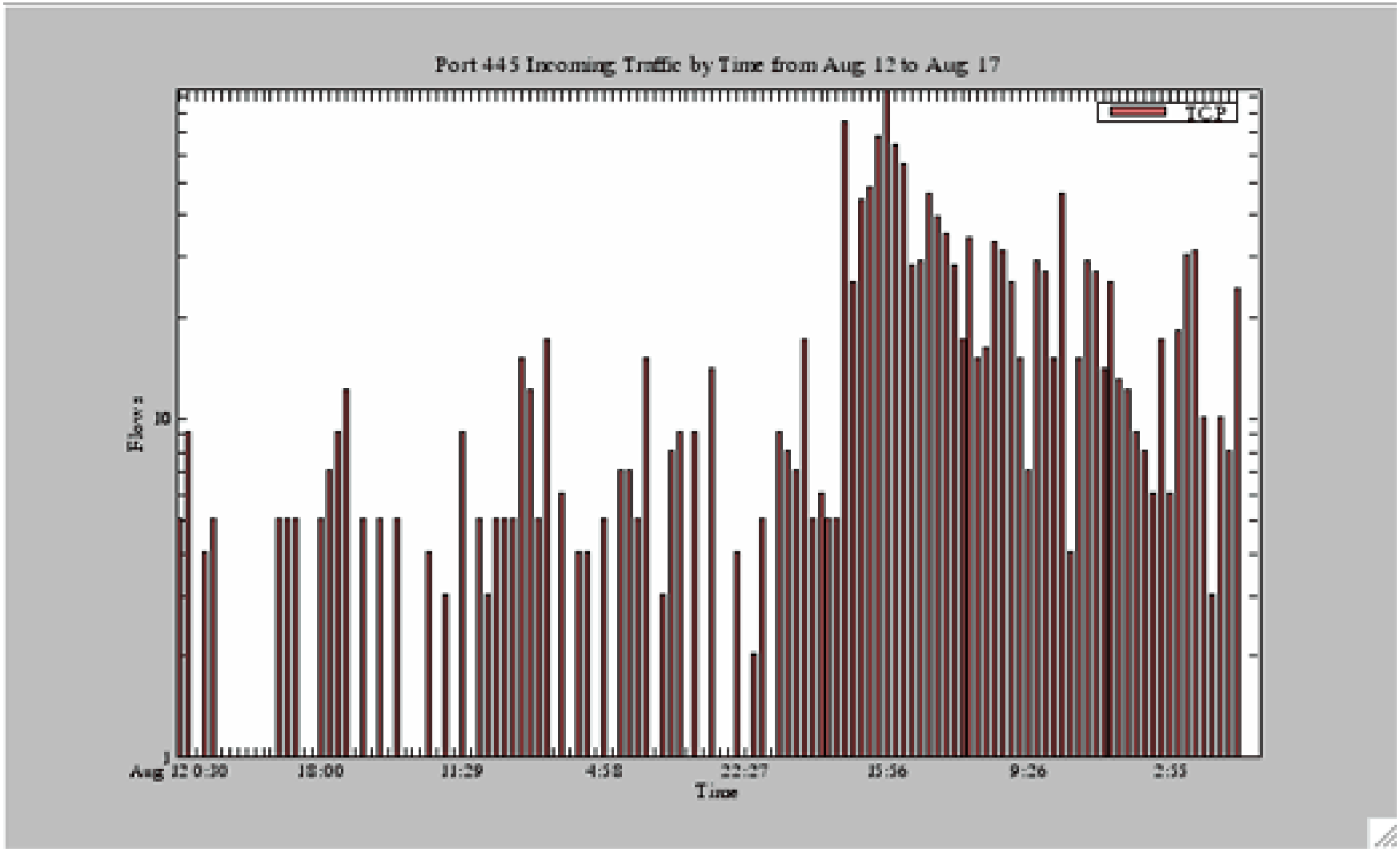

W32.Blaster Worm Propagation observed in the SWITCH Network
unique sources connecting to port 135 TCP
unique sources connecting to port 69 UDP [10x]
unique sources / hour
6000
5000
4000
3000
2000
1000
0
10.08. 00:00
10.08. 12:00
11.08. 00:00
11.08. 12:00
12.08. 00:00
12.08. 12:00
13.08. 00:00
13.08. 12:00
14.08. 00:00
14.08. 12:00
15.08. 00:00
Date and Time (UTC, 2003)

Zotob

(sierpień 2005)

- rozprzestrzeniał się na komputerach z systemem Windows 2000
- atakował przez port 445/TCP
- otwierał tylną furtkę do systemu na porcie 8888/TCP, poprzez który robak uruchamiał na ofierze skrypt FTP – poprzez FTP ściągał pełen kod robaka
- łączył się ze wskazanym serwerem IRC, celem pobrania instrukcji działania
- u zainfekowanego wywoływał ciągły restart systemu

Zotob


Port 445 Incoming Traffic by Time from Aug 12 to Aug 17
TCP
Flows
Aug
12 0:30
18:00
11:29
4:58
22:27
15:56
9:26
2:55
Time

IDS

(**I**ntrusion **D**etection **S**ystems)

Zadania:

- **monitorowanie** ruchu wewnątrz sieci i działań na hoście
- **analiza** bieżąco napływających informacji
- **reakcja :**
- zapis informacji o atakach
- powiadomienia administratora (np. email)
- w typowych sytuacjach przeciwdziałanie

Typy:

- **H**ost-Based **IDS** (HIDS)
(dane pochodzą od hosta)
konieczność instalacji na serwerze

- **N**etwork-Based **IDS** (NIDS)
(dane pochodzą z sieci)
problem w przypadku danych szyfrowanych

- Hybrydowe (NNIDS)

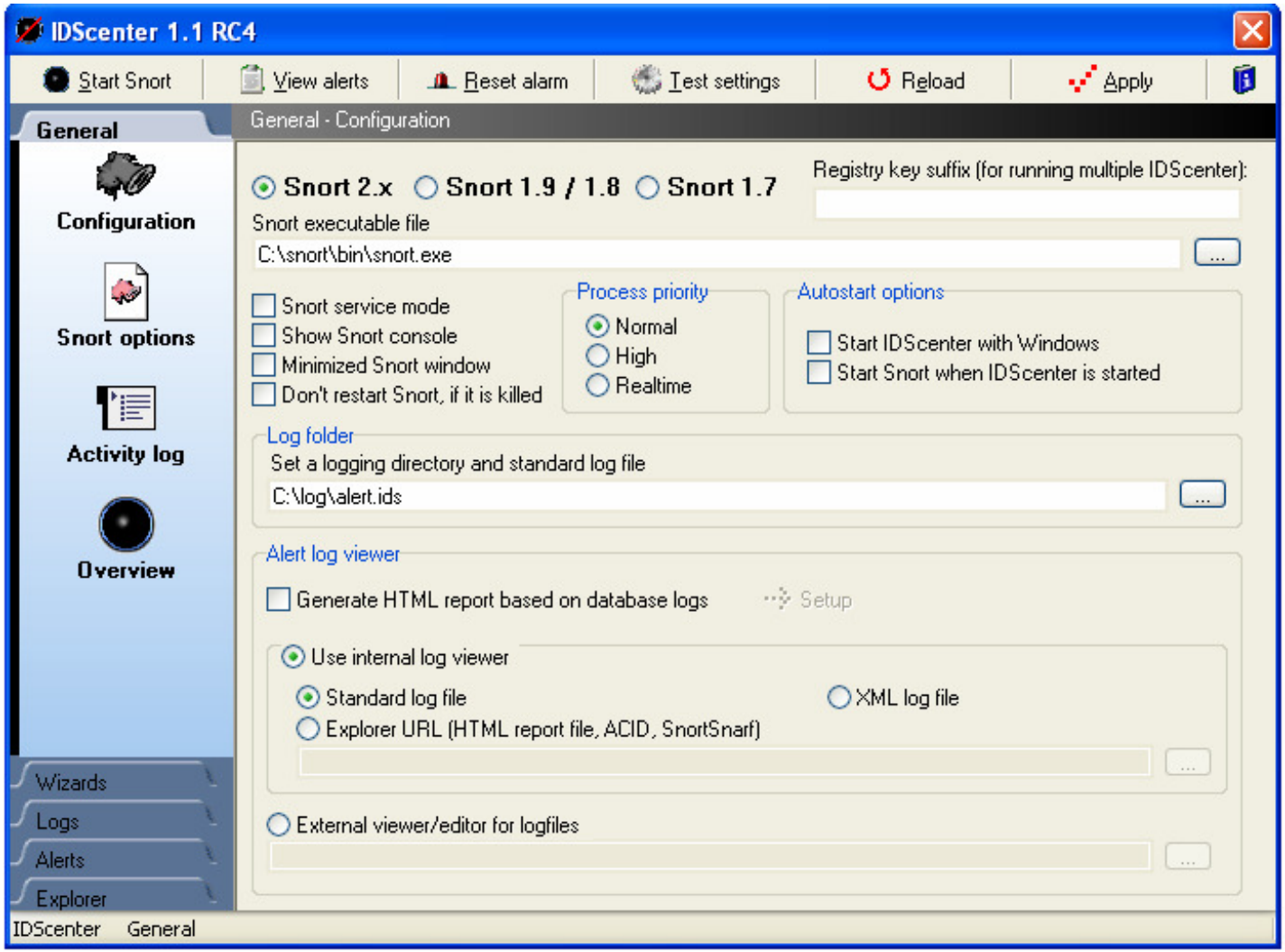
Miary jakości systemów **IDS**

- wykrywalność ataków
- wydajność
- liczba fałszywych alarmów
- wachlarz reakcji
- możliwości dostrajania
- możliwości zarządzania

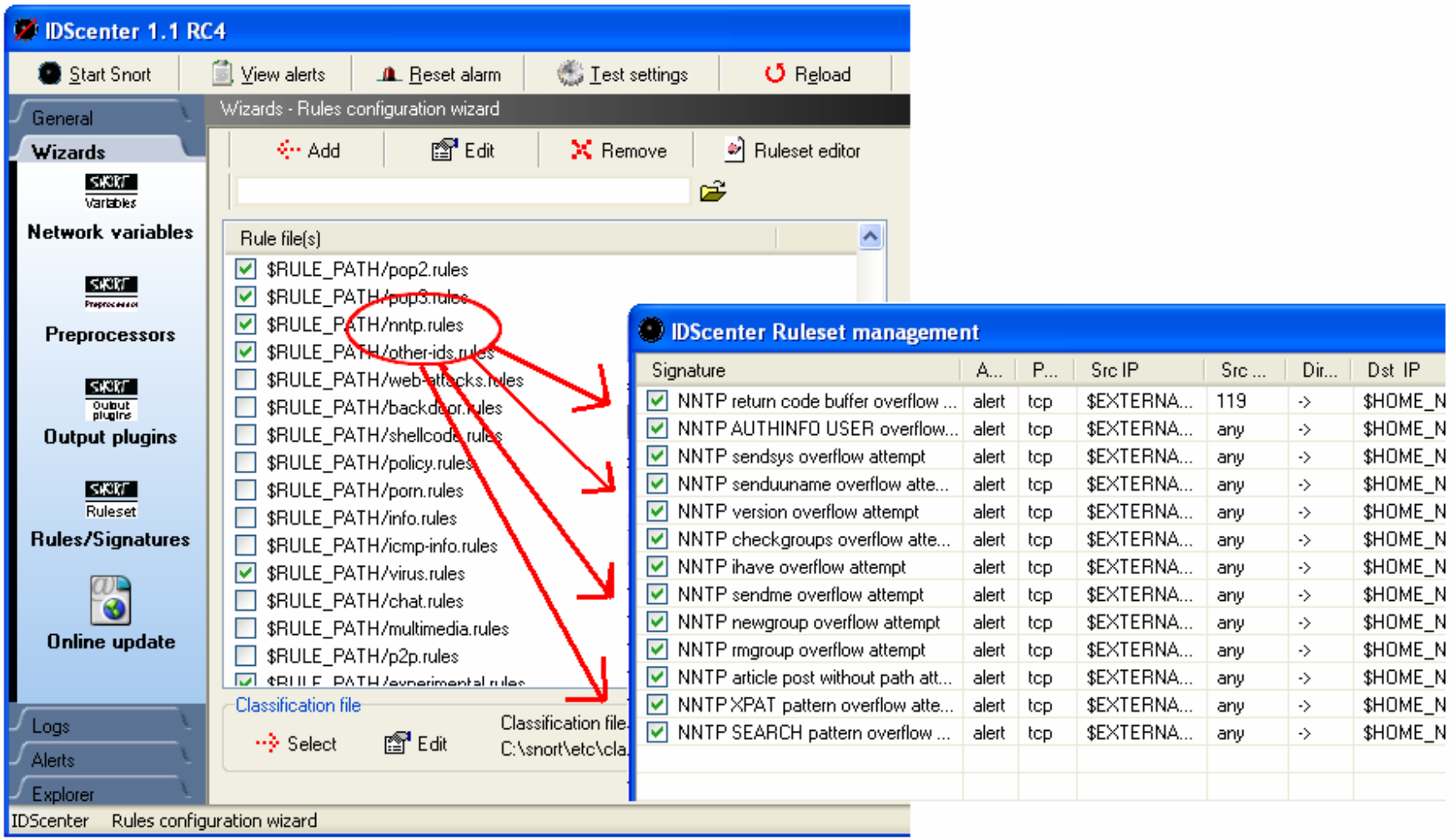
Snort

- działa w czasie rzeczywistym
- dokonuje analizy ruchu i rejestruje pakiety przechodzące przez sieci (oparte na IP/TCP/UDP/ICMP)
- wykrywa przepełnienia bufora, skanowanie portów typu *stealth*, ataki na usługi WWW, SMB, próby wykrywania systemu operacyjnego i wiele innych
- może działać jako sniffer, rejestrator pakietów (w tym zapisywać pakiety w zorganizowanej strukturze katalogów) lub system IDS
- dostępny na licencji wolnego oprogramowania

Snort


IDScenter 1.1 RC4
Start Snort
View alerts
Reset alarm
Test settings
Reload
Apply
General
Configuration
Snort options
Activity log
Overview
Wizards
Logs
Alerts
Explorer
General - Configuration
Snort 2.x
Snort 1.9 / 1.8
Snort 1.7
Registry key suffix (for running multiple IDScenter):
Snort executable file
C:\snort\bin\snort.exe
Snort service mode
Show Snort console
Minimized Snort window
Don't restart Snort, if it is killed
Process priority
Normal
High
Realtime
Autostart options
Start IDScenter with Windows
Start Snort when IDScenter is started
Log folder
Set a logging directory and standard log file
C:\log\alert.ids
Alert log viewer
Generate HTML report based on database logs
Setup
Use internal log viewer
Standard log file
XML log file
Explorer URL (HTML report file, ACID, SnortSnarf)
External viewer/editor for logfiles
IDScenter
General

Snort


IDScenter 1.1 RC4
Start Snort
View alerts
Reset alarm
Test settings
Reload
General
Wizards
Variables
Network variables
Preprocessors
Output plugins
Ruleset
Rules/Signatures
Online update
Logs
Alerts
Explorer
Wizards - Rules configuration wizard
Add
Edit
Remove
Ruleset editor
Rule file(s)
$RULE_PATH/pop2.rules
$RULE_PATH/pop3.rules
$RULE_PATH/nntp.rules
$RULE_PATH/other-ids.rules
$RULE_PATH/web-attacks.rules
$RULE_PATH/backdoor.rules
$RULE_PATH/shellcode.rules
$RULE_PATH/policy.rules
$RULE_PATH/porn.rules
$RULE_PATH/info.rules
$RULE_PATH/icmp-info.rules
$RULE_PATH/virus.rules
$RULE_PATH/chat.rules
$RULE_PATH/multimedia.rules
$RULE_PATH/p2p.rules
Classification file
Select
Edit
Classification file
C:\snort\etc\cla
IDScenter Ruleset management
Signature
A...
P...
Src IP
Src ...
Dir...
Dst IP
NNTP return code buffer overflow ...
NNTP AUTHINFO USER overflow...
NNTP sendsys overflow attempt
NNTP senduuname overflow atte...
NNTP version overflow attempt
NNTP checkgroups overflow atte...
NNTP ihave overflow attempt
NNTP sendme overflow attempt
NNTP newgroup overflow attempt
NNTP rmgroup overflow attempt
NNTP article post without path att...
NNTP XPAT pattern overflow atte...
NNTP SEARCH pattern overflow ...
alert
tcp
$EXTERNA...
119
any
->
$HOME_N
IDScenter
Rules configuration wizard

IPS

(**I**ntrusion **P**revention **S**ystems)

Jedna z definicji:

Systemy chroniące informacje,
a w szczególności ich :

poufność

spójność

dostępność

Przykładowe realizacje:

IDS + …

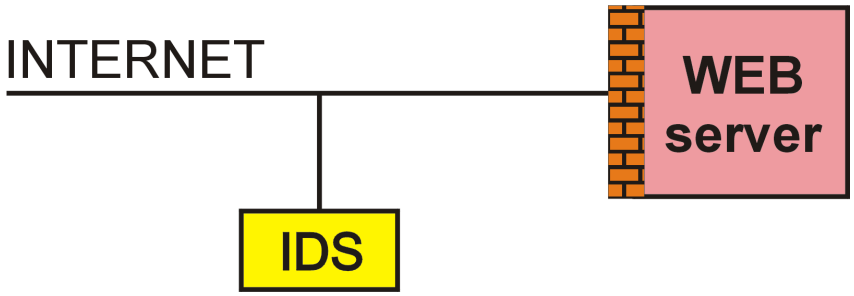
praktycznie każdy
software / hardware
zapobiegający
atakowi

IPS – przykłady realizacji

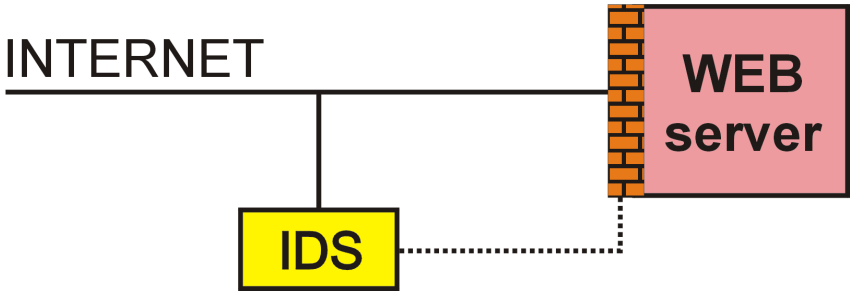
- **IDS** + Firewall
- in-line **IDS**
- przełącznik warstwy 7
- przełącznik hybrydowy
  (IDS + Firewall + przełącznik warstwy 7)
- aplikacja oszukująca

IDS + Firewall

zwykły NIDS :

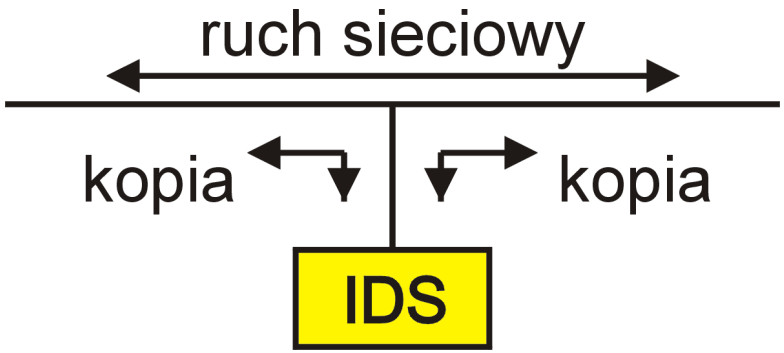


NIDS + Firewall :



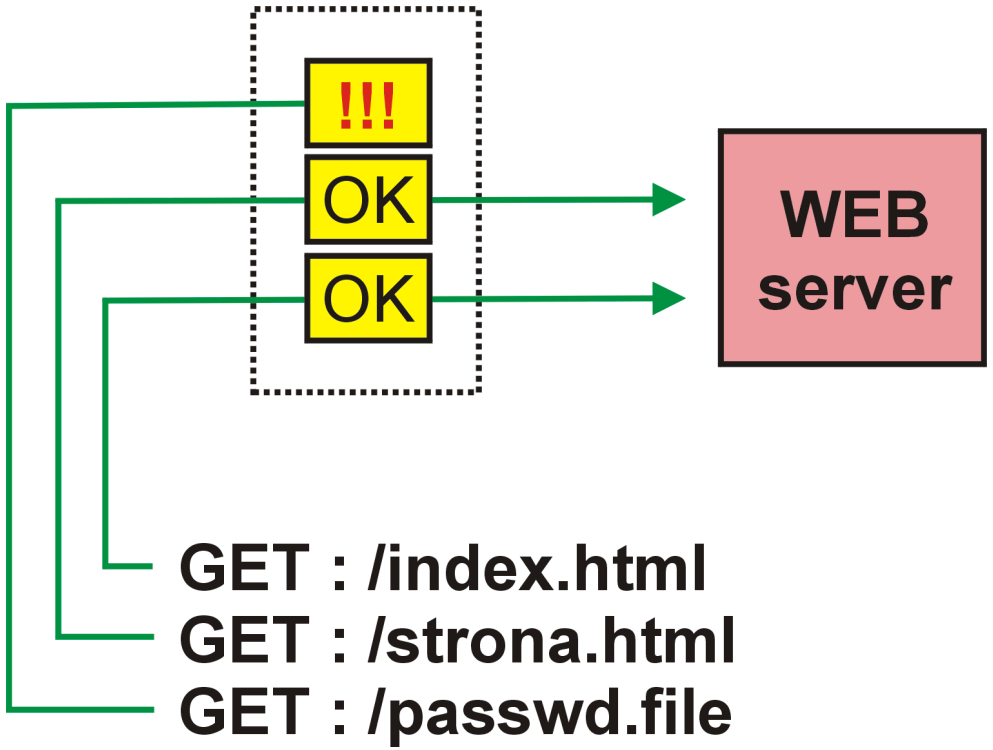
in-line **IDS**

zwykły NIDS :



in-line NIDS :

Przełącznik warstwy 7



IDS vs. **IPS**

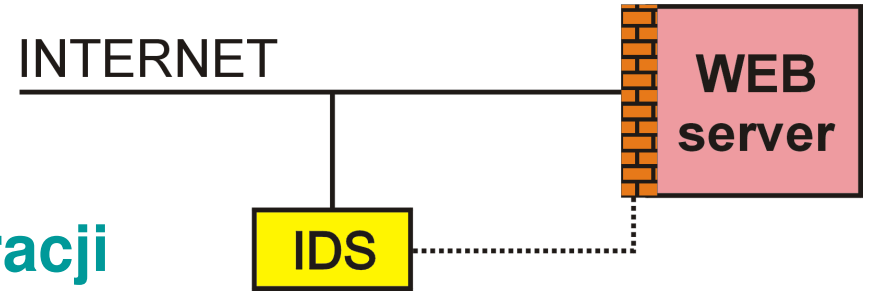
IDS	**IPS**
Pasywny	Aktywny
Opóźniona reakcja	Reakcja natychmiastowa

IPS mogą działać na warstwie 7 (HTTP, FTP, SMTP) w przeciwieństwie do IDS.

Ale uwaga! Każde rozwiązanie ma też swoje wady!

IPS – przykładowe wady

duży problem w razie awarii in-line NIDS



konieczność konfiguracji na każdym z serwerów w przypadku IDS + Firewall

Dziękujemy
za uwagę!