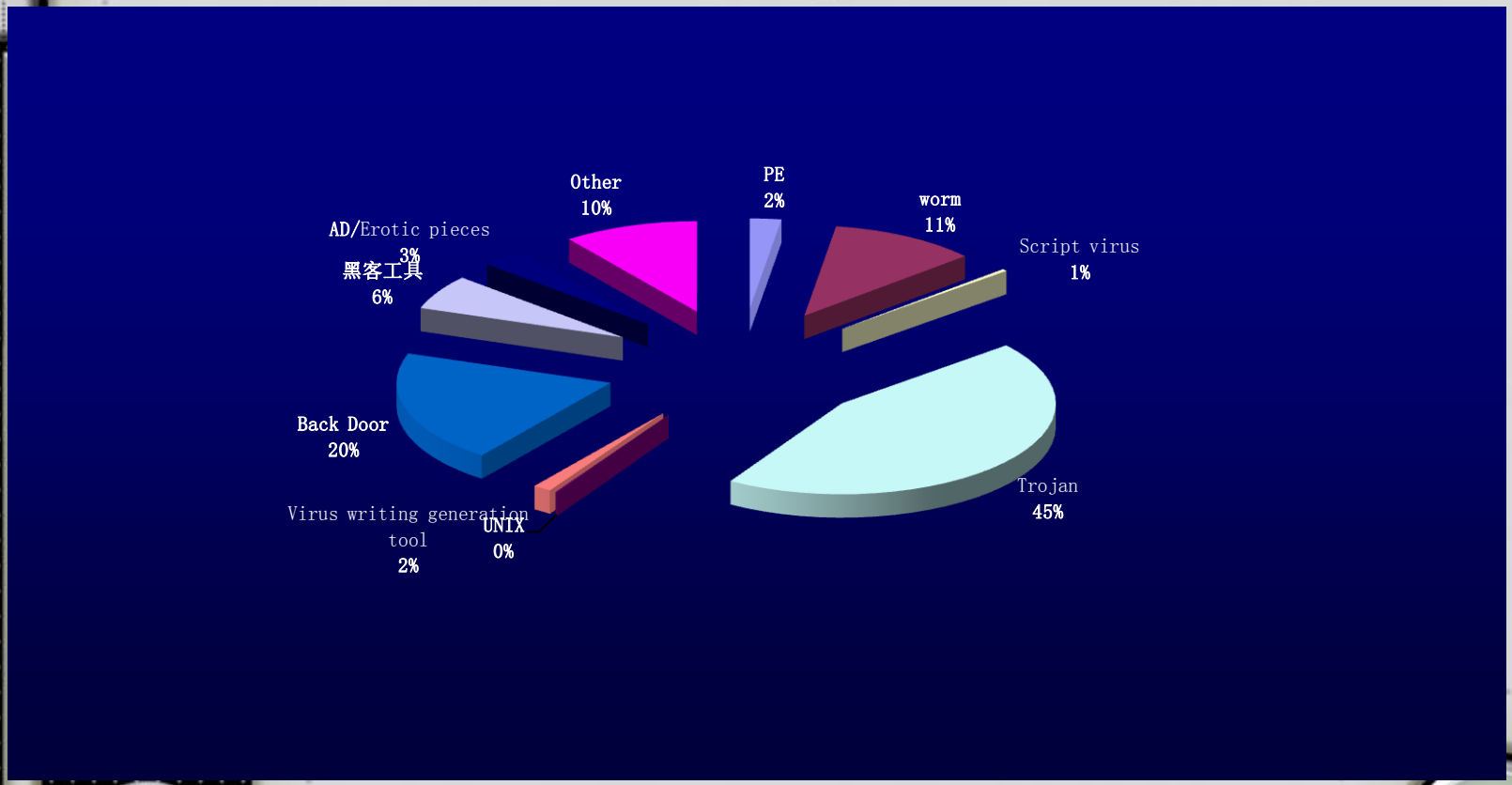
Virus Detection System
VDS

seak@antiy.net

Outline

- The virus trends of 2004
- Qualities of an IDS
- Mechanisms of a VDS
- Data processing

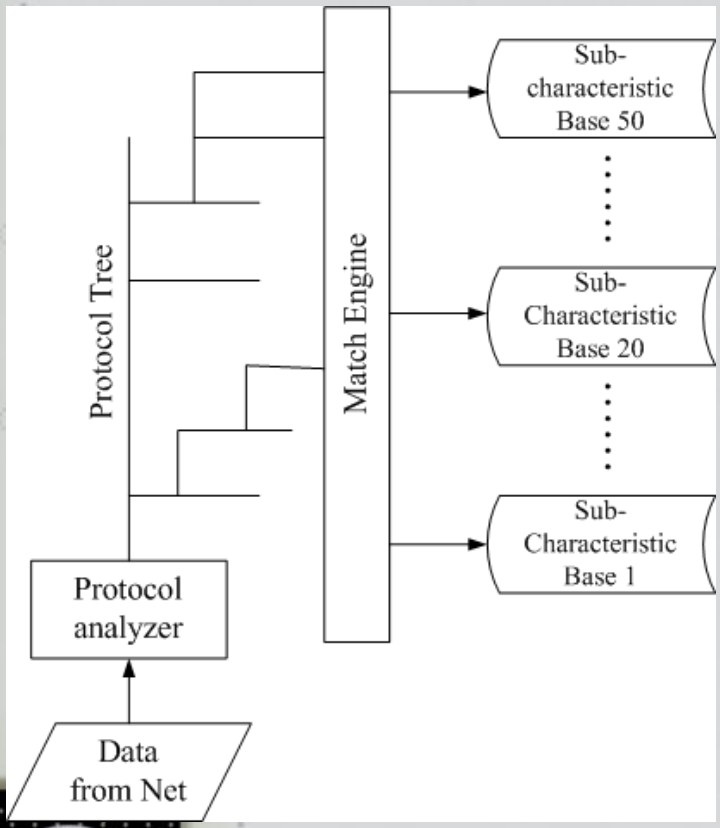
20047 new kinds of virus in 2004



Outline

- The virus trends of 2004
- Qualities of an IDS
- Mechanisms of a VDS
- Data processing

How a traditional IDS works



- Meticulous protocol analysis
- Lightweight rule set
- No more than 500 records in a rule set.

Unitary software designing

- Unitary design: In the case of dealing with an extensive complicated incident, we should classify the events and unify one or more of the processing modules by using an extensible data structure and data set.
- AV Ware: Scan target object's divergence.
- IDS: Protocol's divergence.

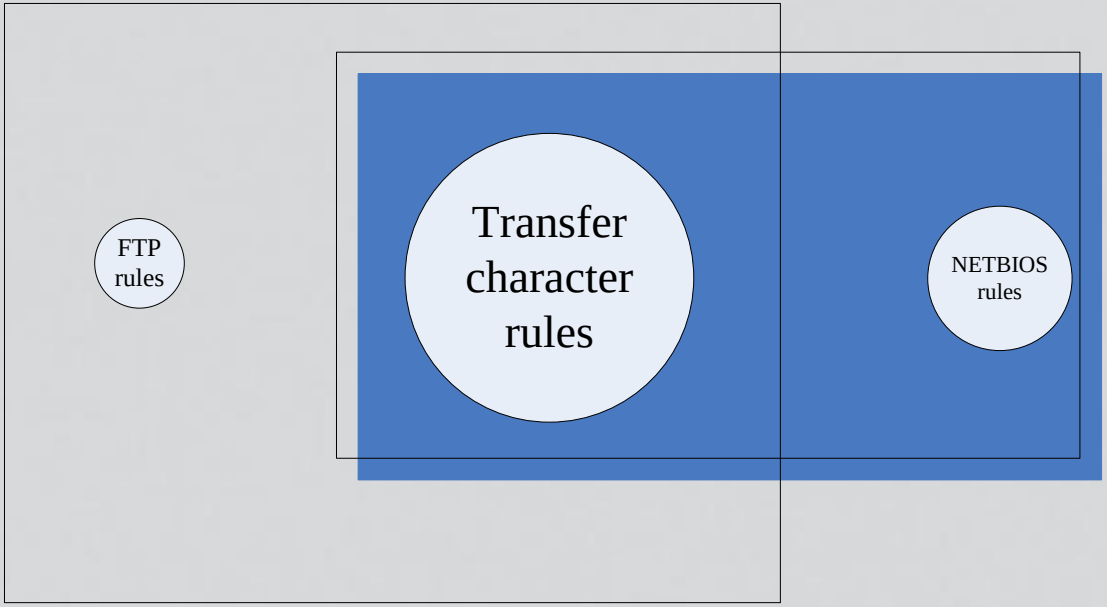
AVML and Snort

- Echo virus(id=”B00801”;type=”Backdoor”;os=”Win32”;format=”pe”;name=”bo”;version=”a”;size=”124928”;Port_listen=on[31337];content=|81EC0805000083BC240C05000000535657557D148B8424240500008BAC24200500005 0E9950500000F85800500008B|;delmark=1)

- alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"Backdoor.bo.a Upload"; content: |81EC0805000083BC240C05000000535657557D148B8424240500008BAC24200500005 0E9950500000F85800500008B |;)

- alert tcp $EXTERNAL_NET any -> $HOME_NET 139 (msg:"Backdoor.bo.a Copy"; content: |81EC0805000083BC240C05000000535657557D148B8424240500008BAC24200500005 0E9950500000F85800500008B |;)。

Redundant scans caused by divergence



Rule set scaling pressure

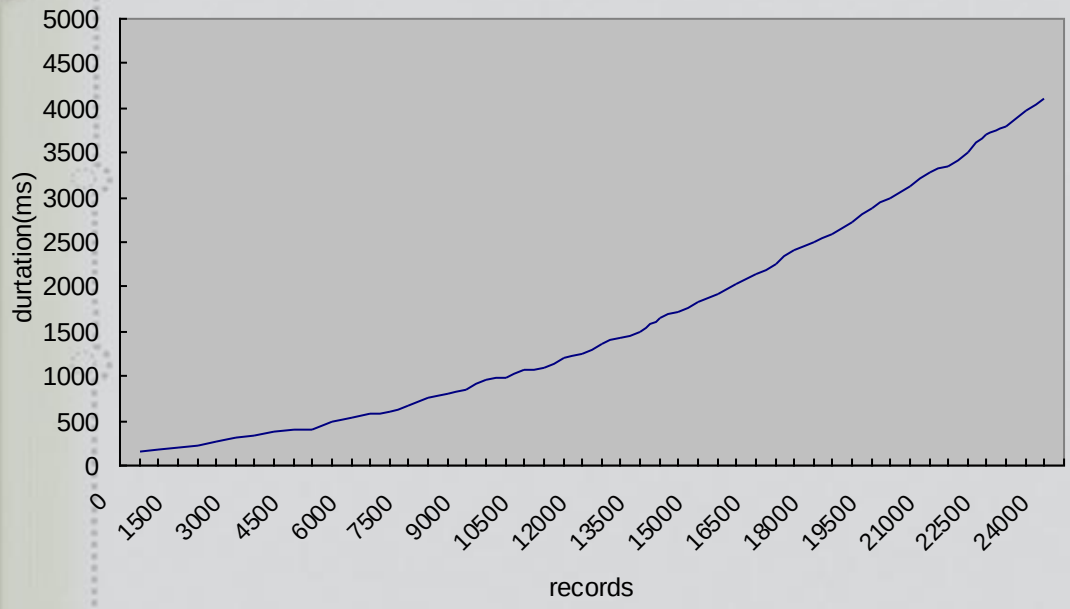
type	quantity
Email worm	2807
IM-worm	172
P2P-worm	1007
IRC-worm	715
Other worm	675
total	5376

- Besides worms, there are over 20,000 Trojans, Backdoors, etc… which transfer over the network.
- The corresponding rule quantity may exceed 30,000 records.

Outline

- The virus trends of 2004
- Qualities of an IDS
- Mechanisms of a VDS
- Data processing

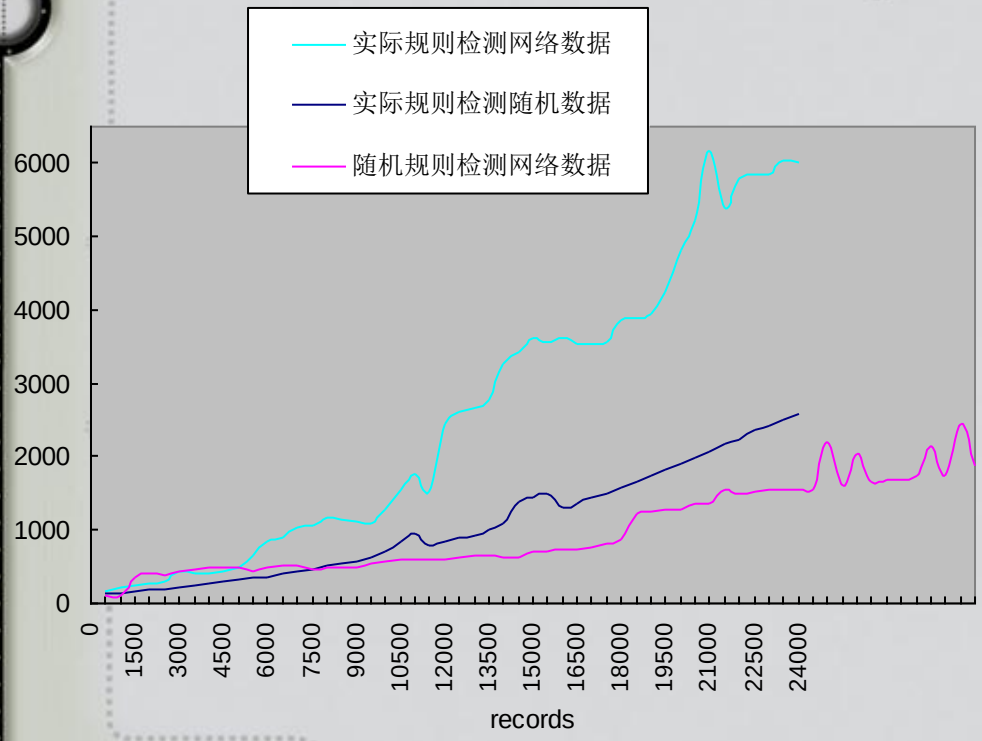
Algorithm optimization（1）



When the quantity of rules is less than 6,000, it is not obvious that time increases linearly with record count. But after about 10,000 records, that begins to change, causing a sudden drop in performance up until it is simply unavailable。

- The influence of record quantity on record matching time

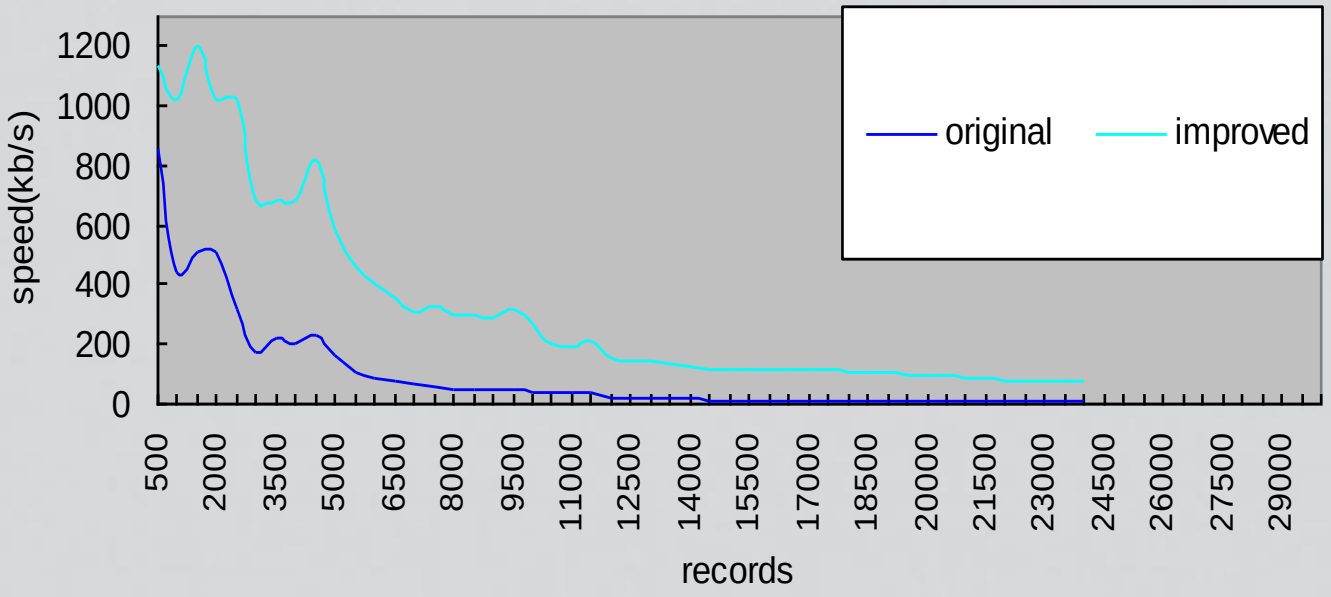
Algorithm optimization （2）



- The scanning speed is also affected by the data being matched and the quality of the patterns.

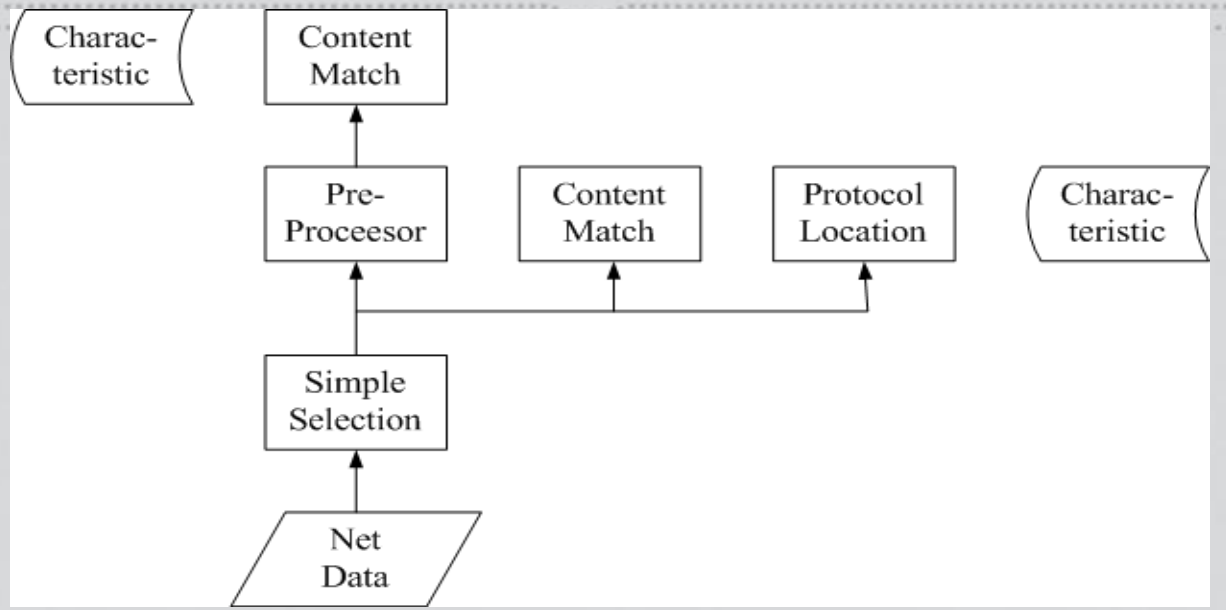
Scan methods' and data objects' influence on the speed

Algorithm optimization （3）



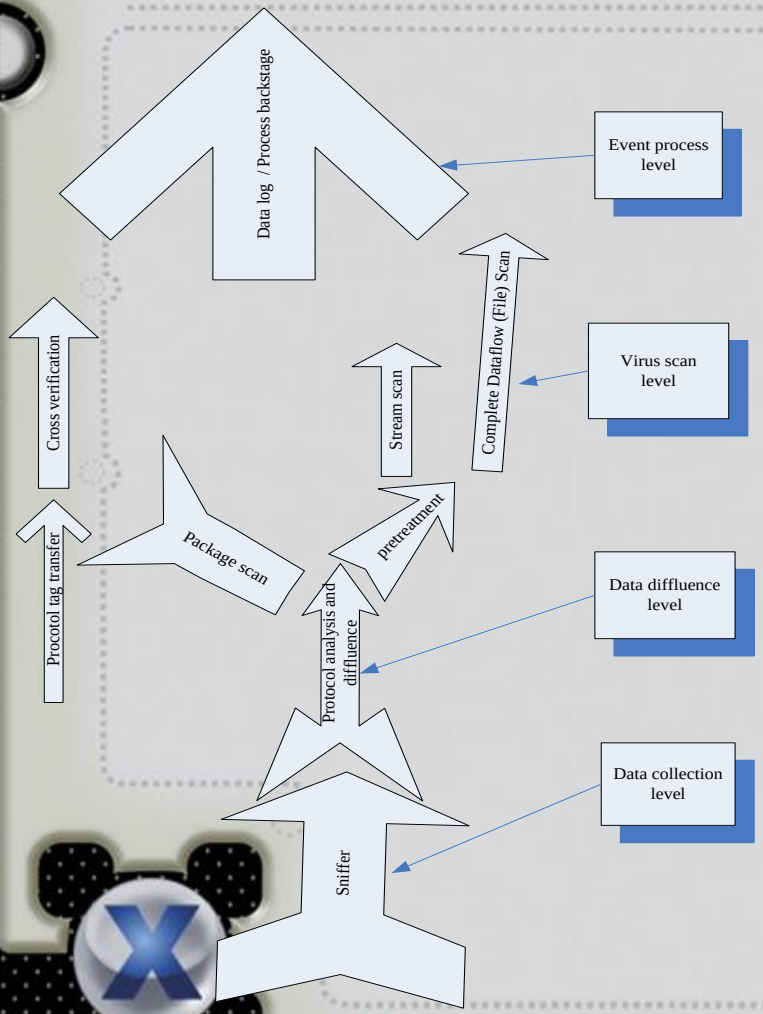
- Influence on efficiency caused by limiting the approximation of the virus' characteristics

Key method of designing VDS



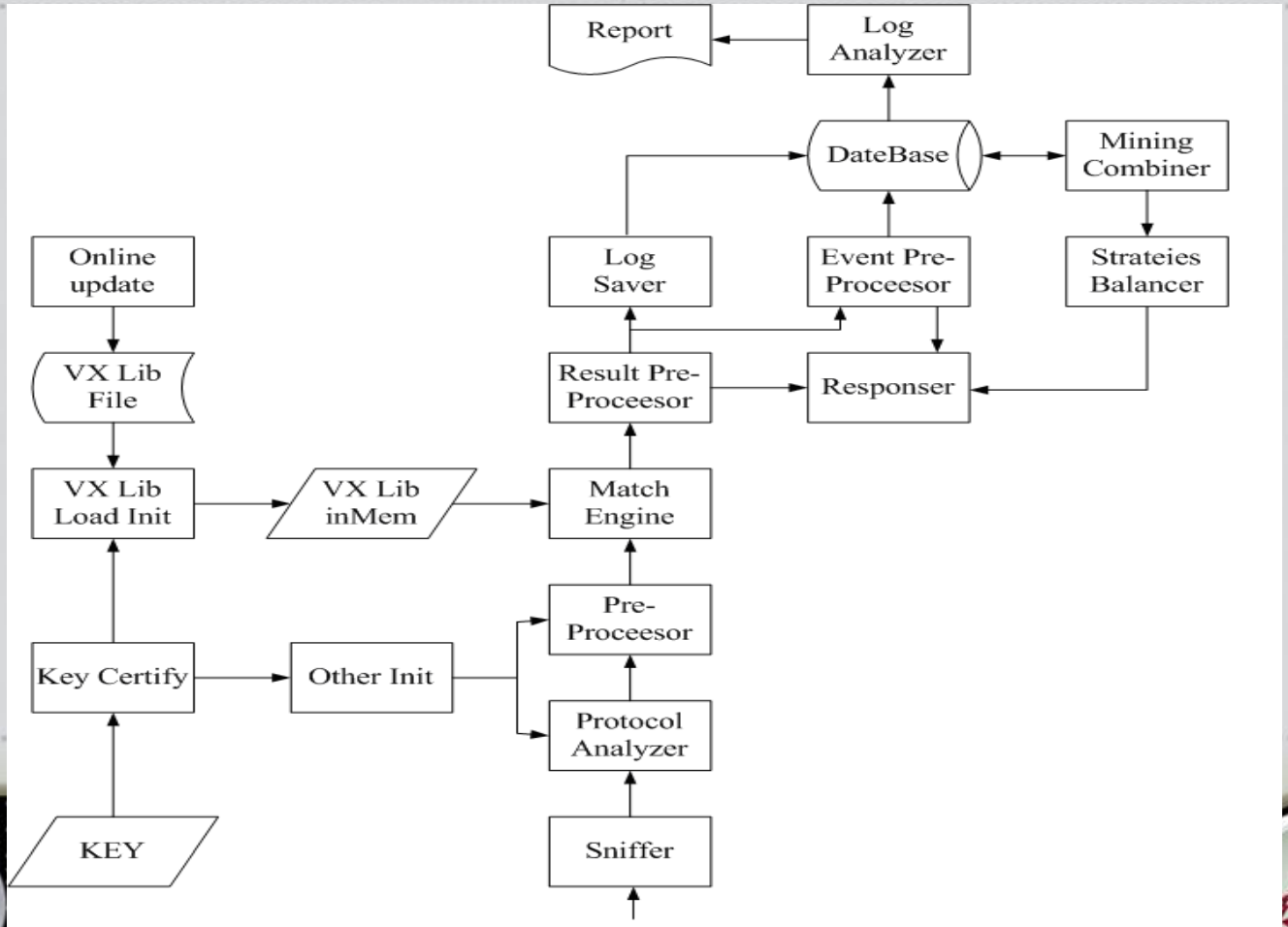
- The Unitary Model focuses on matching speed and matching granularity — matching is of foremost importance.
- Network traffic data is classified into three types：data matched on the binary level, data needing pre-treatment and data needing specific algorithms。

Data flow direction and the Level of virus detection

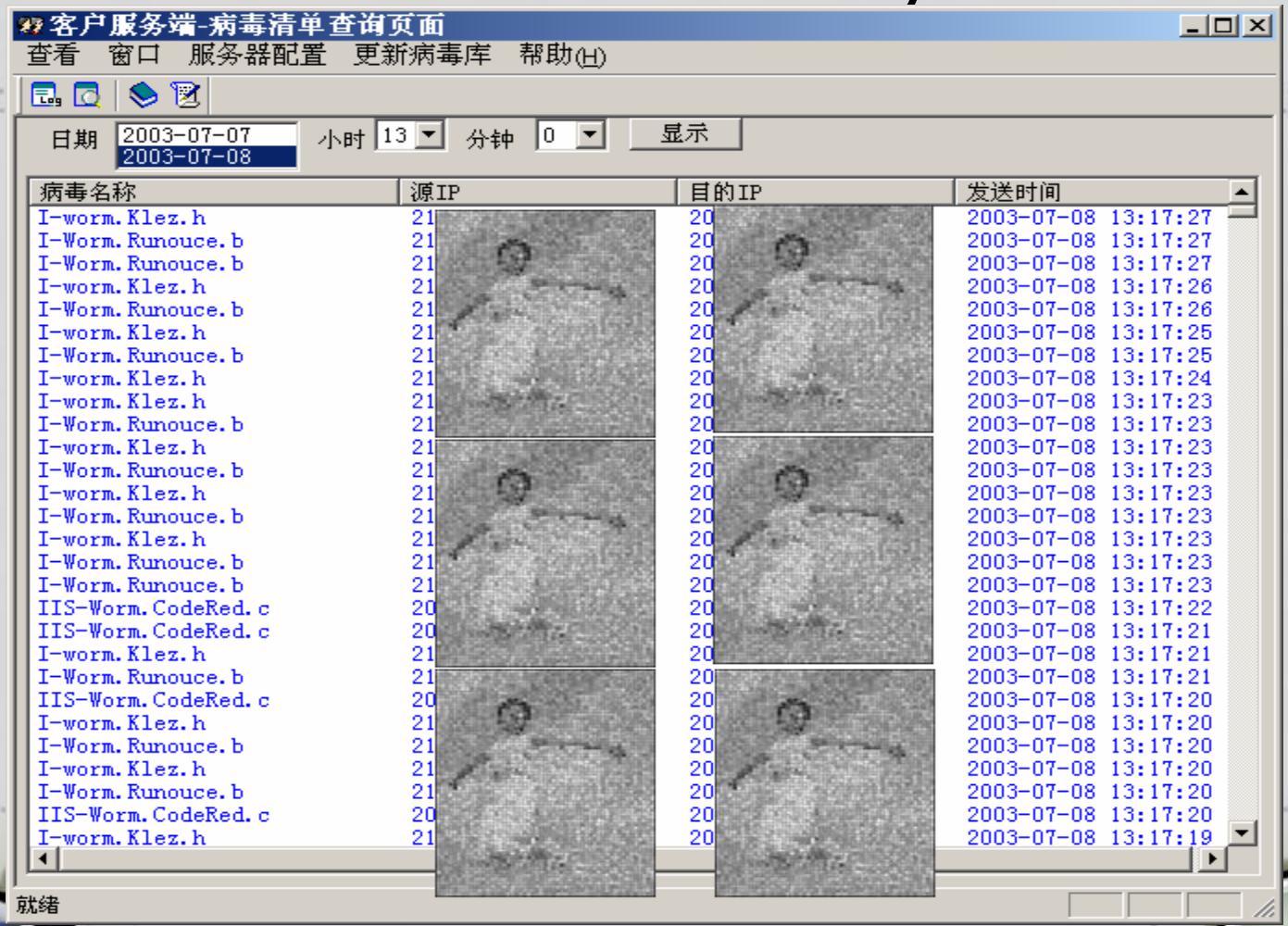


- Divided into 4 levels: collection, divergence, detection and processing
- Provides package scanning, incomplete data scanning And complete data scanning.

System structure



Data efficiency



Virus data output from Harbin Institute of Technology on July 8 , 2003.

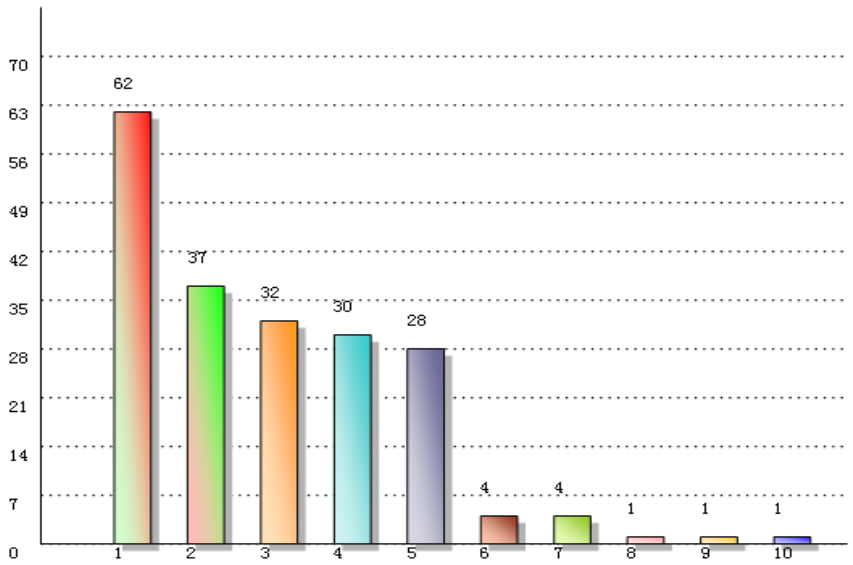
Statistics from the 26th week of 2005

2005年26周邮件蠕虫监测结果统计报告

检出次数排行榜

名次	病毒名称	进入内网比例	检出次数	病毒流量(byte)	感染列表
1	Email-Worm.Win32.Bagle.af	100%	62	0	受感染主机 受攻击主机
2	Email-Worm.Win32.LovGate.ad	100%	37	0	受感染主机 受攻击主机
3	Email-Worm.Win32.LovGate.ae	0%	32	0	受感染主机 受攻击主机
4	Email-Worm.Win32.LovGate.w	100%	30	0	受感染主机 受攻击主机
5	Email-Worm.Win32.LovGate.w	0%	28	0	受感染主机 受攻击主机
6	Email-Worm.Win32.NetSky.c	100%	4	0	受感染主机 受攻击主机
7	Email-Worm.Win32.LovGate.q	100%	4	0	受感染主机 受攻击主机
8	Email-Worm.Win32.Zafi.d	100%	1	0	受感染主机 受攻击主机
9	Email-Worm.Win32.Bagle.af	0%	1	0	受感染主机 受攻击主机
10	Email-Worm.Win32.NetSky.z	100%	1	0	受感染主机 受攻击主机
		总计	200	0	

检出次数统计图



Unknown virus forewarning system

发现病毒体传输次数排行榜：		
名次	病毒名	发现次数
1	[illegible]	[illegible]
2	I-Worm.UNKnow	2548
3	[illegible]	[illegible]
4	I-Worm.Nimda	2
5	Backdoor.Netbus.160.a	1
6	Trojan.Win32.HDBreaker	1

- Detected an unknown worm (I-Worm.Unknow) increasing notably on June 5, 2003. On June 6 it was shown to be the virus I-worm.sobig.f.

Outline

- The virus trends of 2004
- Qualities of an IDS
- Mechanisms of a VDS
- Data processing

Event Processing (1)

- Detection Events Description Language (DEDL).
- We use descriptors to define standard formats for network events and make them support other formats
- Defined elements: event type, event ID, source IP, target IP, event time, and so on. More than 20 such key elements.

- **Processing methods**
- Tech-based Internal combine
- Parallel combine
- Analysis-based Parallel combine
- Radiant combine
- Convergence combine
- Chain combine

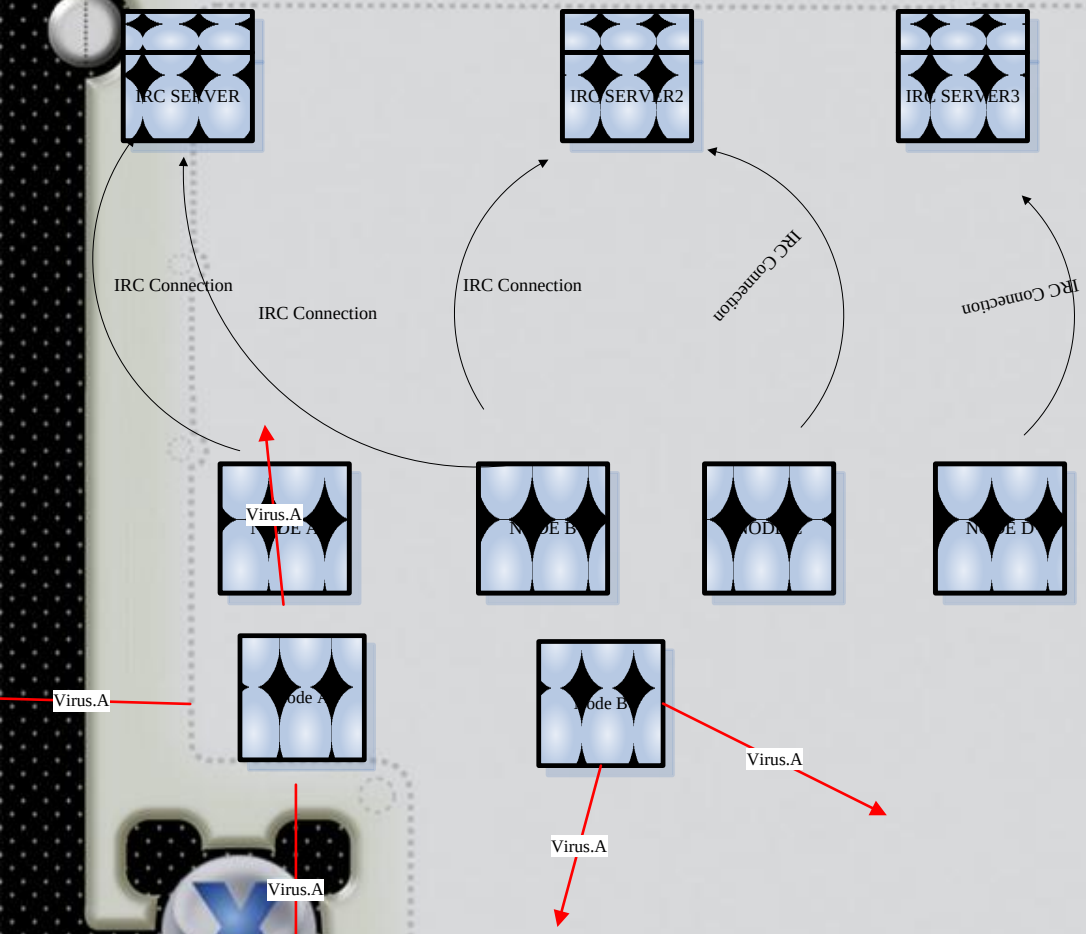
Event Processing (2)

If existNet_Action(RPC_Exploit)[IP(1)->IP(2);time(1)]
Net_Action(RPC_Exploit) [IP(2)->IP(3) ;time(2)]
and
time(2)>time(1)
than
Net_Action(RPC_Exploit) [IP(1)-> IP(2) -> IP(3)]

Behavior Classifications

DEDL events	AVML diagnostic behavior regulations
Net_Action(act)[IP(1),IP(2):445; ;time(1)] Net_Action(act)[IP(1),IP(3):445; ;time(1)] .... Net_Action(act)[IP(1),IP(12):445; ;time(1)] Net_Action(Trans,Worm.Win32.Dvldr)[IP(1)->IP(12);time(1)]	Virus_act_lib Virus seek(id=″W02872″;dport=139,445;trans=netbios)

Data processing



Thoughts

- Network virus monitoring has been explored academically and productively. It has now expanded into a new technology with its own direction.
- The path of virus defense leads us to the world of freedom.