uVALUE

17th Annual FIRST Conference

Proposal for the experimental environment for Network Worm infection

2005/06/29

Masato Terada
Graduate School of Science and Technology, Keio University
Hitachi Incident Response Team, Hitachi Ltd.

HITACHI
Inspire the Next

Opening

The code analysis and simulation of network worm infection are useful methods to evaluate how it spreads and its effects. Also, it is important to evaluate the retrieval behavior of network worm infection in experimental environment for complementing a code analysis.

This presentation describes a prototype of experimental environment for network worm infection and actual data on network worm infection.

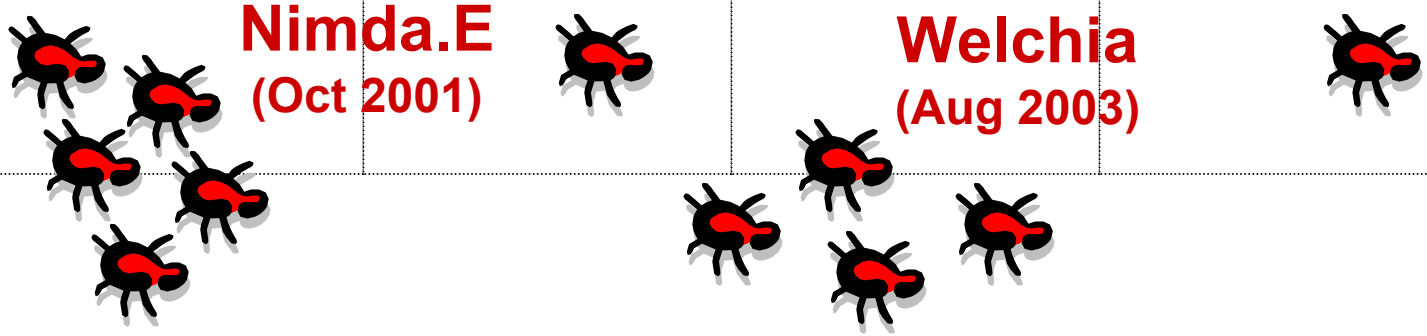
Contents

HITACHI
Inspire the Next

1 Network-Based Malware strikes again and again and again…

Hitachi Incident Response Team

2001	2002	2003	2004	2005
IIS/sadmind (May 2001)	Slapper (Sep 2002)		Sasser.A-F (May 2004)	
Code Red I (Jul 2001)		Slammer (Jan 2003)		
Code Red II (Aug 2001)		Code Red III (Mar 2003)		
Nimda (Sep 2001)		Blaster (Aug 2003)		
Nimda.E (Oct 2001)		Welchia (Aug 2003)		

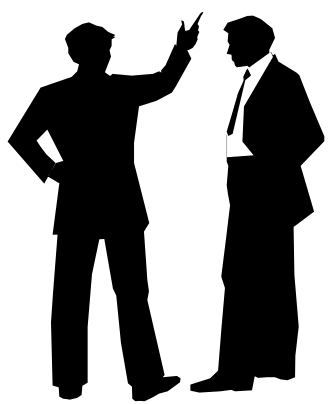


Hitachi Incident Response Team

Code analysis and simulation of network worm infection are useful methods to evaluate how it spreads and its effects.

A bug in infection algorithm or the way to implement a random number generator etc. could affect retrieval behavior of network worm infection.

Unfortunately there is no actual, measured data on network worm infection for public use.



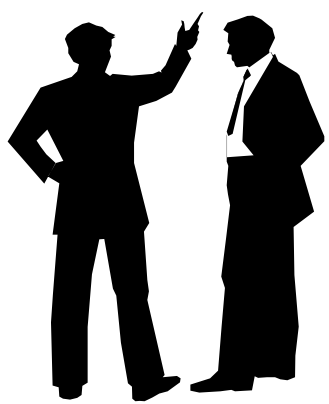
Hitachi Incident Response Team

Code analysis and simulation of network worm infection are useful methods to evaluate how it spreads and its effects.

It is useful to evaluate the network worm behavior in experimental environment, don't you think?

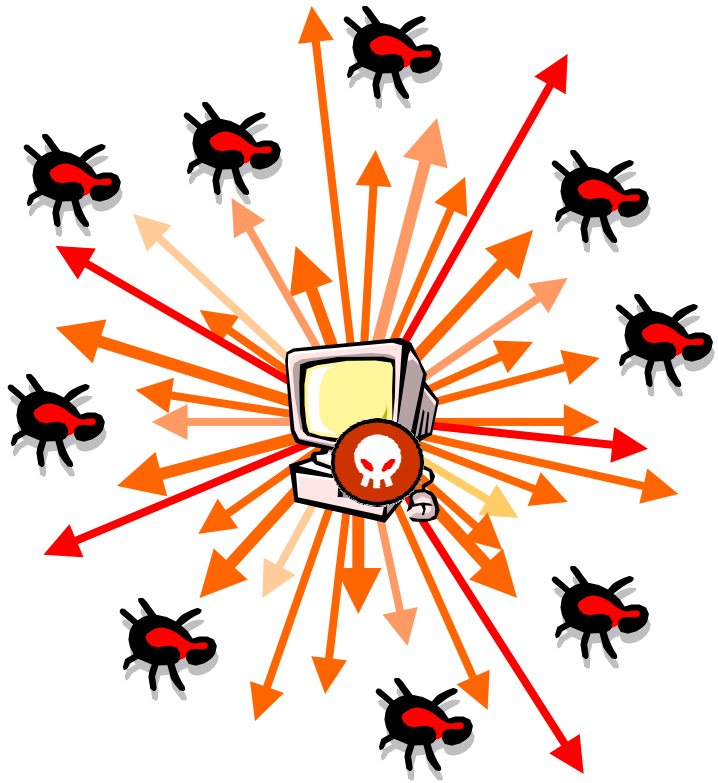
But how do we construct an experimental environment ?

What can we get by using an experimental environment ?



Our proposal for the experimental environment

- **For retrieval behavior**
  - Address block ratio of IP addresses retrieved by network worms
- **For infection behavior**
  - Port numbers used by network worms



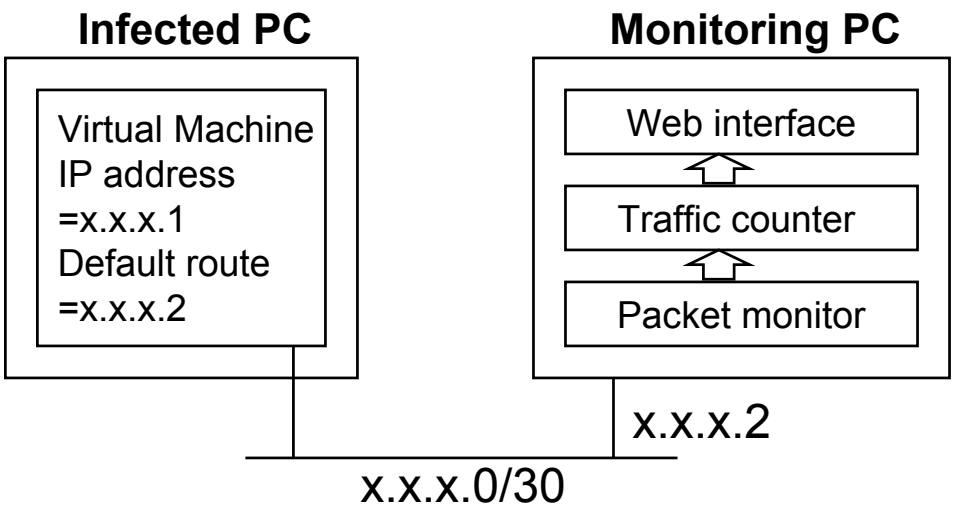
HIRT Hitachi Incident Response Team

Requirements for the experimental environment

- It doesn't need to use a special device, and is a small-scale, readily-available system with just enough hardware/software
- It provides information for building countermeasures to prevent network worm infection.
  - Address block ratio of IP addresses retrieved by network worms
  - Port numbers used by network worms
- It makes it possible to efficiently verify infection behavior of network worms

Our proposal for the experimental environment = Prototype for retrieval behavior =

It doesn't need to use a special device, and is a small-scale system with just sufficient HW/SW.



Infected PC

Item	Description
Base HW	Dell PowerEdge1400 Pentium III, Memory 256MB
Base OS	Microsoft Windows 2000 Server Service Pack 4
VM HW	Memory Guest memory size 160MB VM total memory 176MB
VM OS	Microsoft Windows 2000 Server Windows XP Professional

Monitoring PC

Item	Description
Base HW	IBM Thinkpad 2609-93J Pentium III, Memory 192MB
Base OS	Red Hat Linux 7.3

Our proposal of the experimental environment = Result example of retrieval behavior (Web Interface)=

Hitachi Incident Response Team

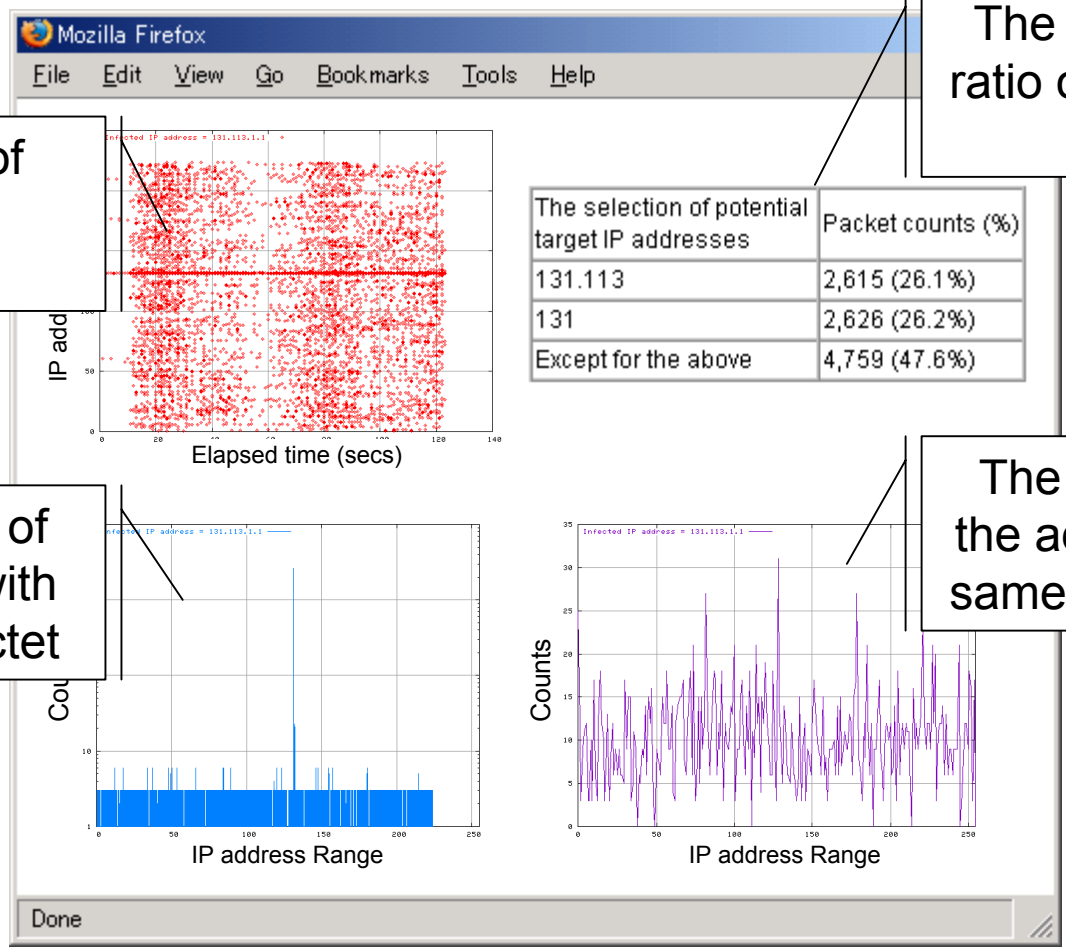
◆ Characteristics of retrieval behavior

The mapping of retrieved IP addresses

The address block ratio of IP addresses retrieved

The distribution of the addresses with the same first octet

The distribution of the address with the same first-two octets



The selection of potential target IP addresses	Packet counts (%)
131.113	2,615 (26.1%)
131	2,626 (26.2%)
Except for the above	4,759 (47.6%)

Sasser.C

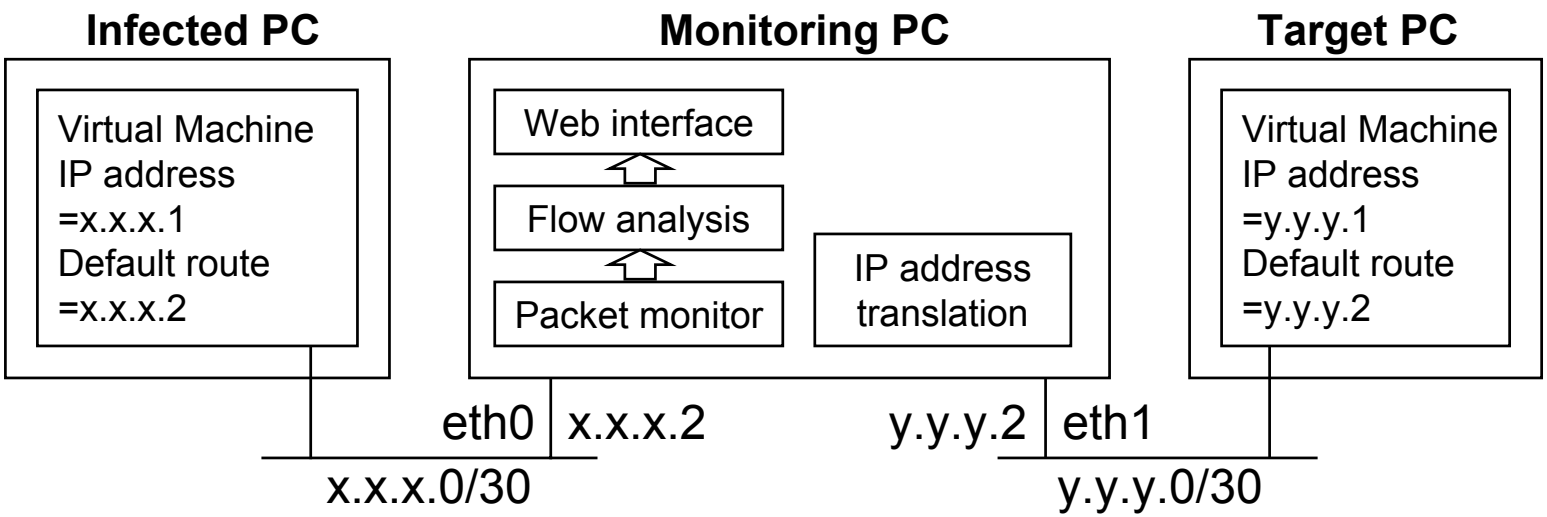
Our proposal of the experimental environment = Prototype for infection behavior =

Hitachi Incident Response Team

It doesn't need to use a special device, and is a small-scale system with just sufficient HW/SW.

Target PC

Item	Description
Base HW	Hitachi FLORA Pentium 4, Memory 1GB
Base OS	Microsoft Windows XP Professional Service Pack 1
VM HW	Memory Guest memory size 512MB VM total memory 528MB
VM OS	Microsoft Windows XP Professional



Our proposal of the experimental environment = Example result of infection behavior (Web Interface)=

Hitachi Incident Response Team

- Destination port number used by the network worm
- Destination port number series used by the network worm and its frequency

Number of packets captured

Start time of the infection activity

Series of destination port numbers

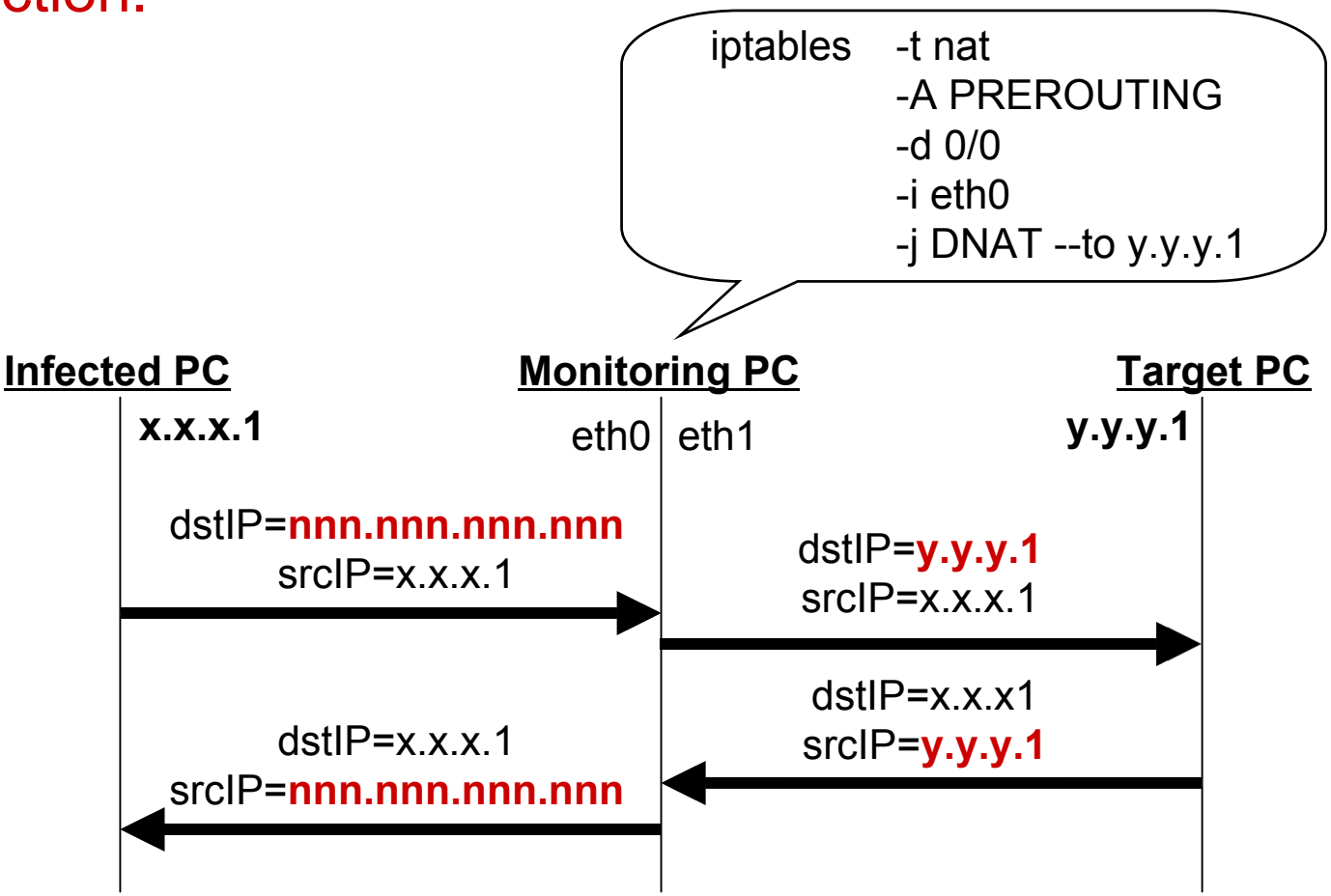
Total packet counts	53782
Infection activity start time	1 0.000000 Packet No, Elapsed Time

The series of port numbers	Counts	The logs of first appearance packet Line1: Packet No, Elapsed time, src IP address, dst IP address, Protocol, src PT number, dst PT number Line2: Flag information
445/TCP	2	602 7.882561 131.113.1.1 149.144.49.64 TCP 1096 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
445/TCP 9996/TCP	693	1 0.000000 131.113.1.1 131.113.98.125 TCP 1053 > 445 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 169 2.262588 131.113.1.1 131.113.98.125 TCP 1065 > 9996 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
5554/TCP 1033/TCP	1	236 2.867330 192.168.1.1 131.113.1.1 TCP 1032 > 5554 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 248 2.895472 131.113.1.1 192.168.1.1 TCP 1069 > 1033 [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460

Sasser.C

Our proposal of the experimental environment = IP address translation: DNAT =

- Our prototype uses “Linux iptables DNAT (Destination Network Address Translation)” as IP address translation function.



Our proposal of the experimental environment = Flow analysis =

The flow analysis function has two steps: extraction of the packet of interest that has made the first appearance ("the first appearance packet") and then identification of the destination port number series.

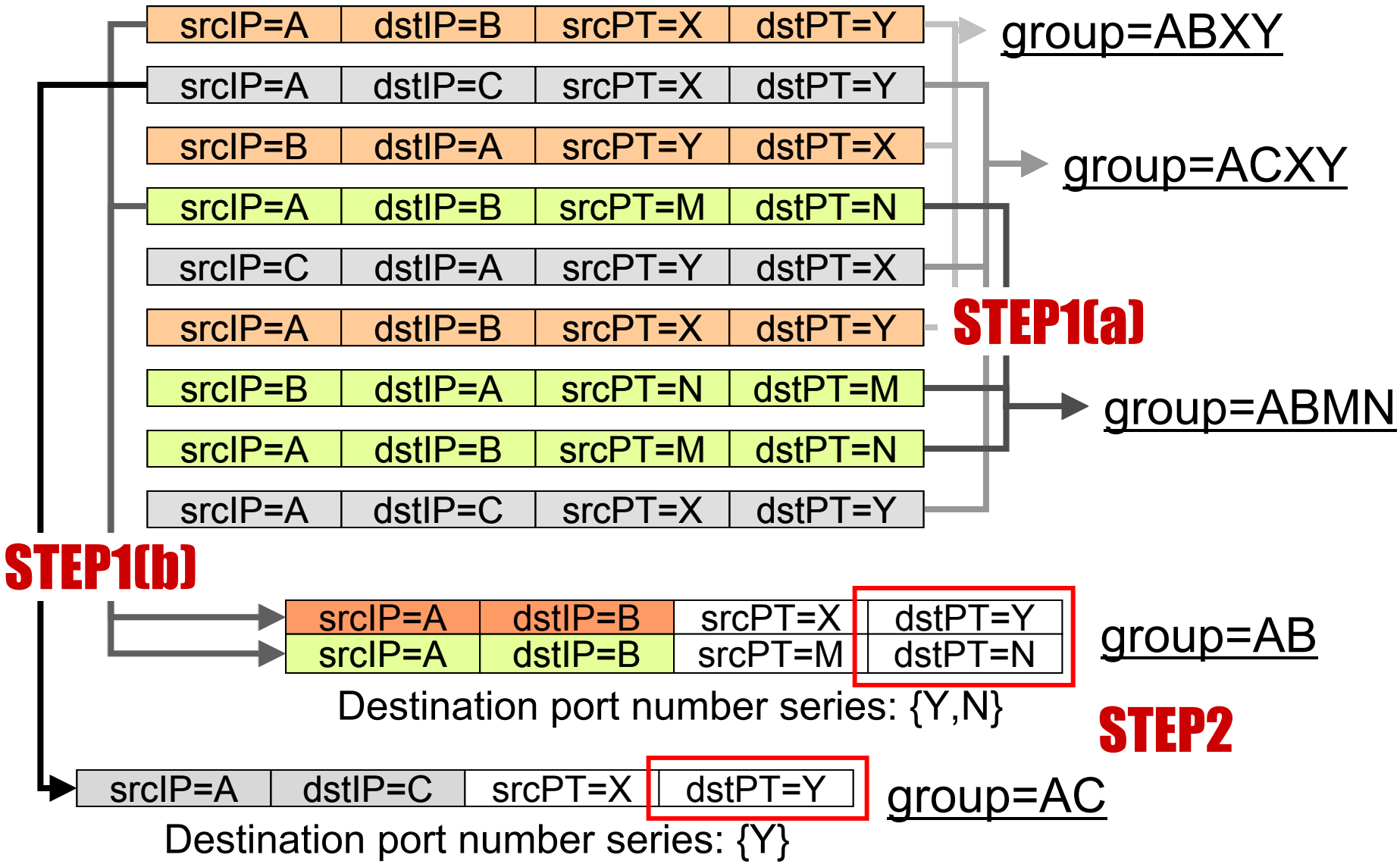
◆ STEP1: Extraction of the first appearance packet

- (a) Divide packets into groups according to the src/dst IP address pairs and the src/dst port number pairs.
- (b) Extract the first appearance packet from each group and identifies the destination port number used in network worm infection.

◆ STEP2: Determination of the destination port number series

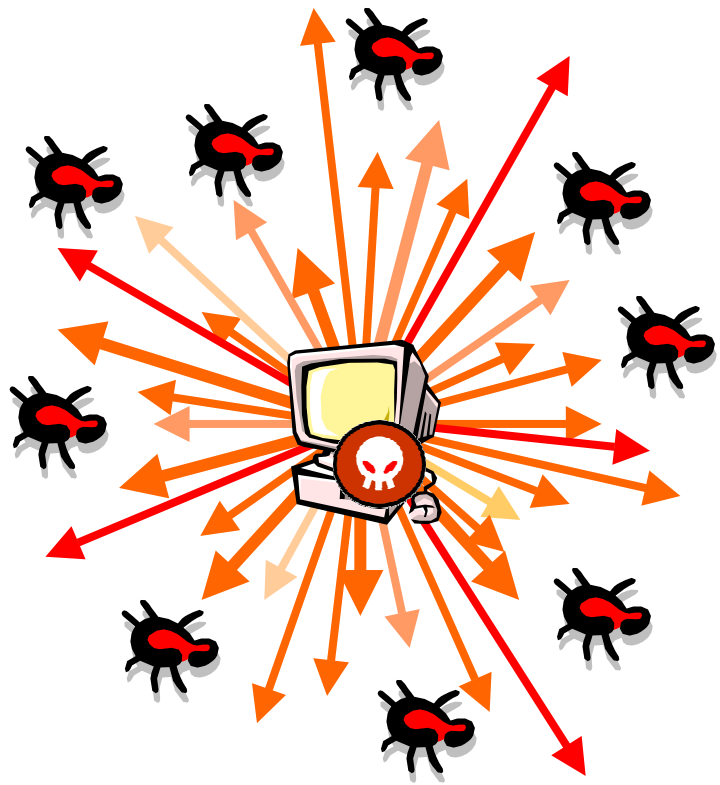
- Divide the first appearance packets extracted in STEP 1 into groups according to the src/dst IP address pairs again and determines the destination port number series.
- Summarize the destination port number series you've identified.

2 Our proposal of the experimental environment = Flow analysis (cont.)=



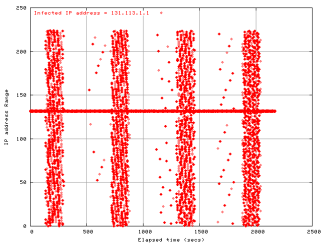
Verification by using the experimental environment

- **Retrieval behavior**
  - Code Red III, Nimda.E, Blaster, Slammer, Sasser.B, Sasser.C
- **TCP retransmission behavior**
  - Code Red III, Nimda.E, Blaster, Sasser.B, Sasser.C
- **Infection behavior**
  - Blaster, Welchia, Sasser.B, Sasser.C



Classification of retrieval behavior

The dependence on address block ratio



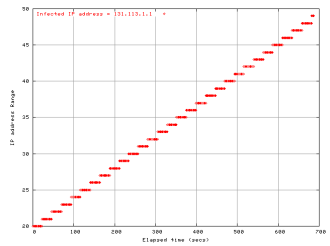
Periodic

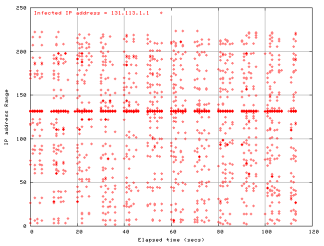
Dependent

Nimda.E

CodeRed III
Sasser.B
Sasser.C

Blaster

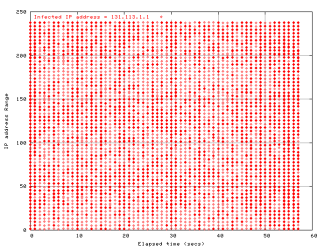




The selection type

Random

Sequential
(one by one)

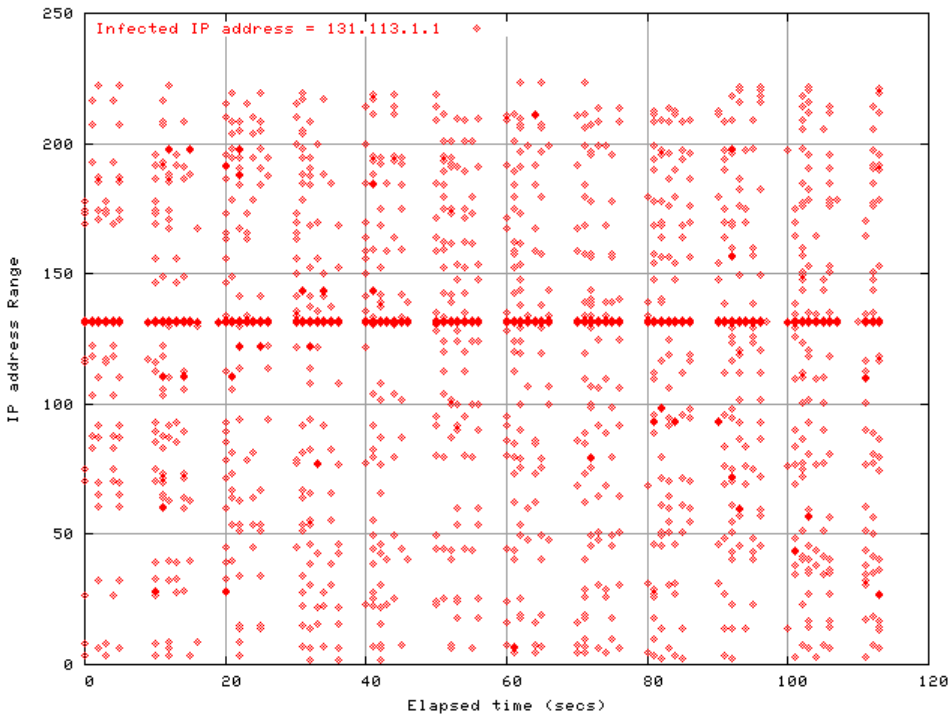


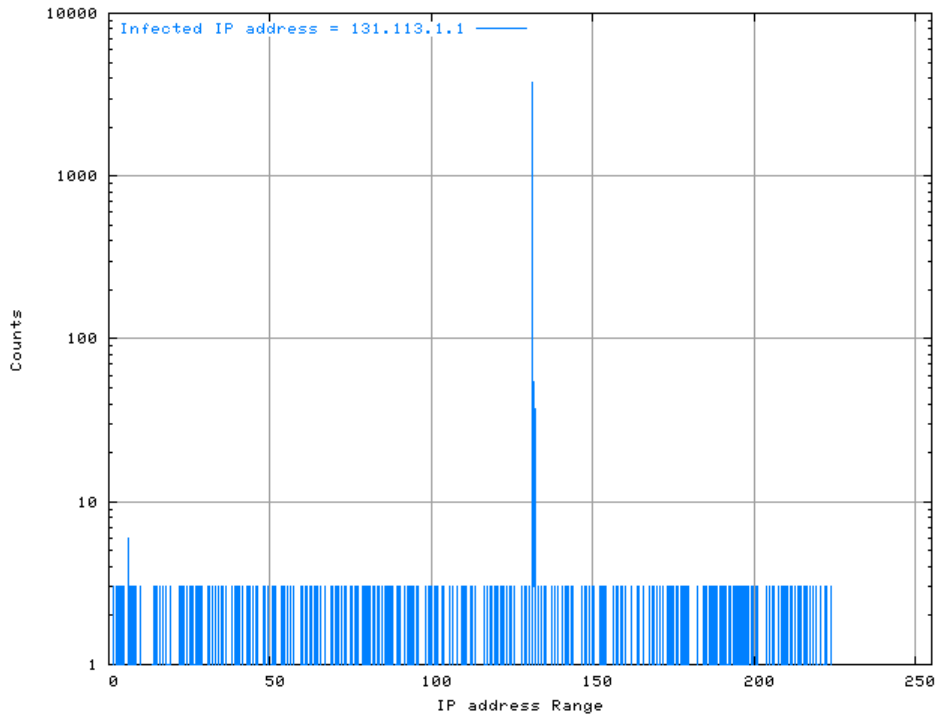
Slammer

Independent

Retrieval behavior
= Code Red III (80/tcp) =

Selection of IP address	Experiment Data	Code Analysis
The same first two octets	37.7%	37.5%
The same first octet	50.8%	50.0%
Others	11.5%	12.5%
The average of 3 trials (10,000 packets/trial).		

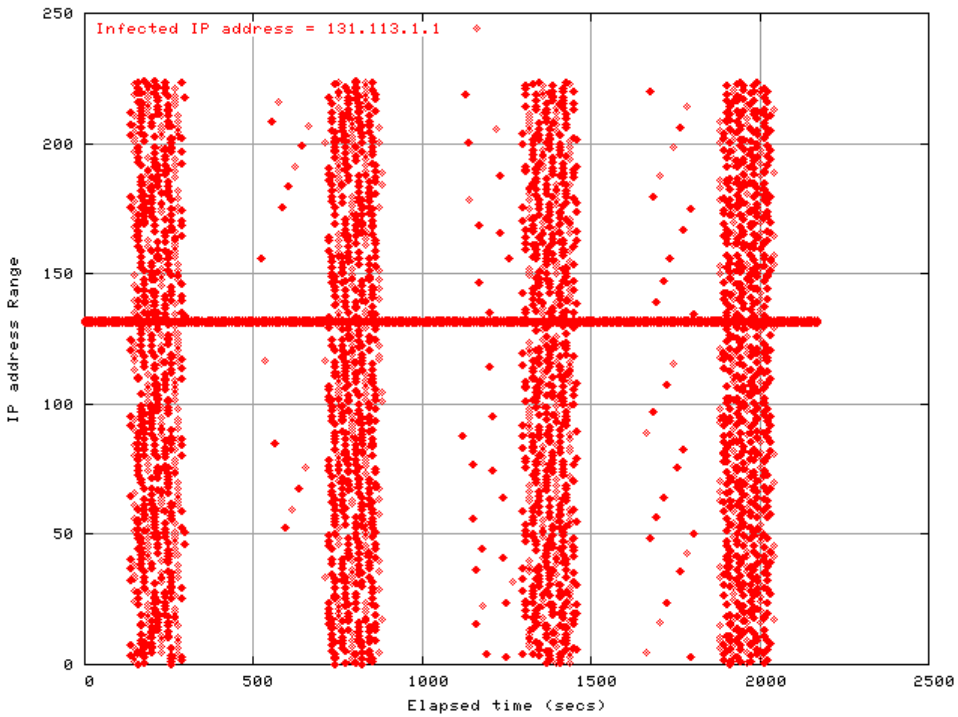


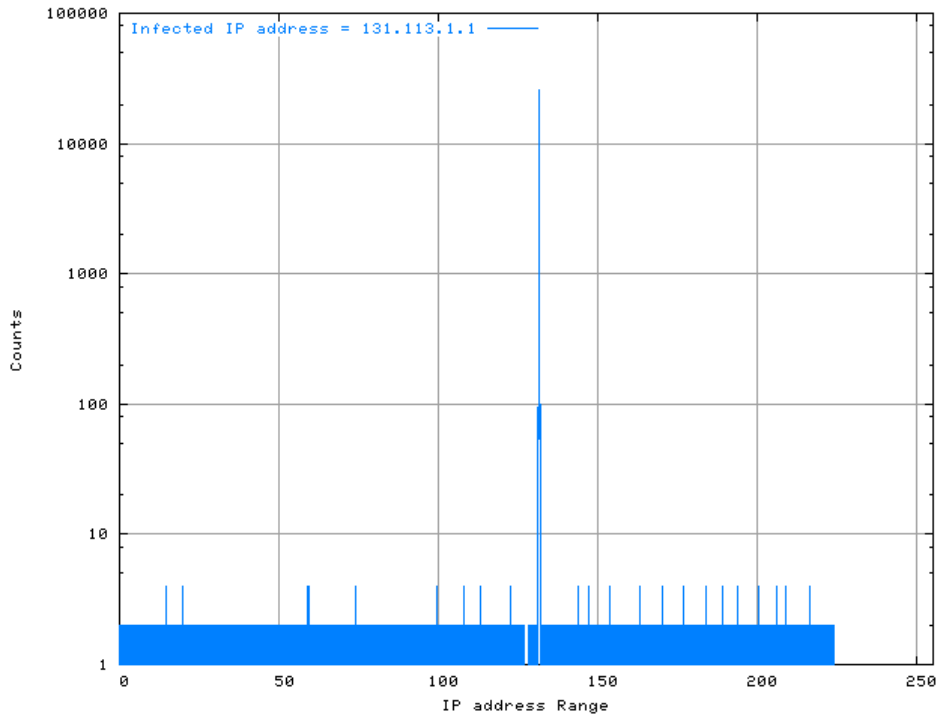


Plot above: from the time observation started to the time # of pkts reached 10,000.

Retrieval behavior = Nimda.E (80/tcp) =

Selection of IP address	Experiment Data	Code Analysis
The same first two octets	50.9%	50%
The same first octet	38.8%	25%
Others	10.3%	25%
The average of 9 trials (10,000 packets/trial).		



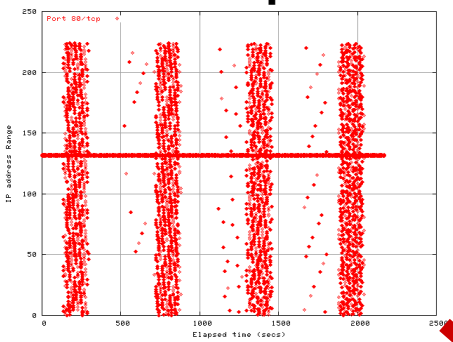


Plot above: from the time obs. started to the time # of pkts reached 51,261.

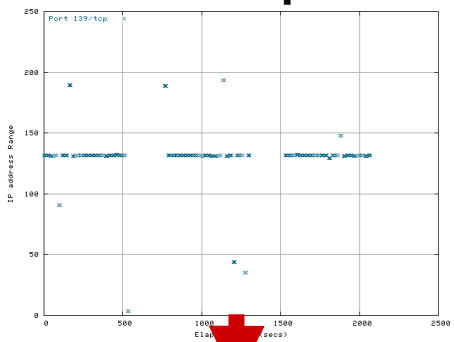
Retrieval behavior
= Nimda.E (80/tcp, 139/tcp, 445/tcp) =

HIRT Hitachi Incident Response Team

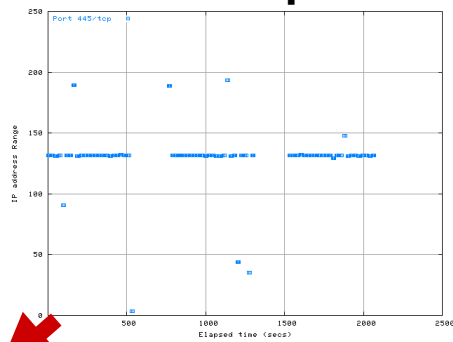
80/tcp

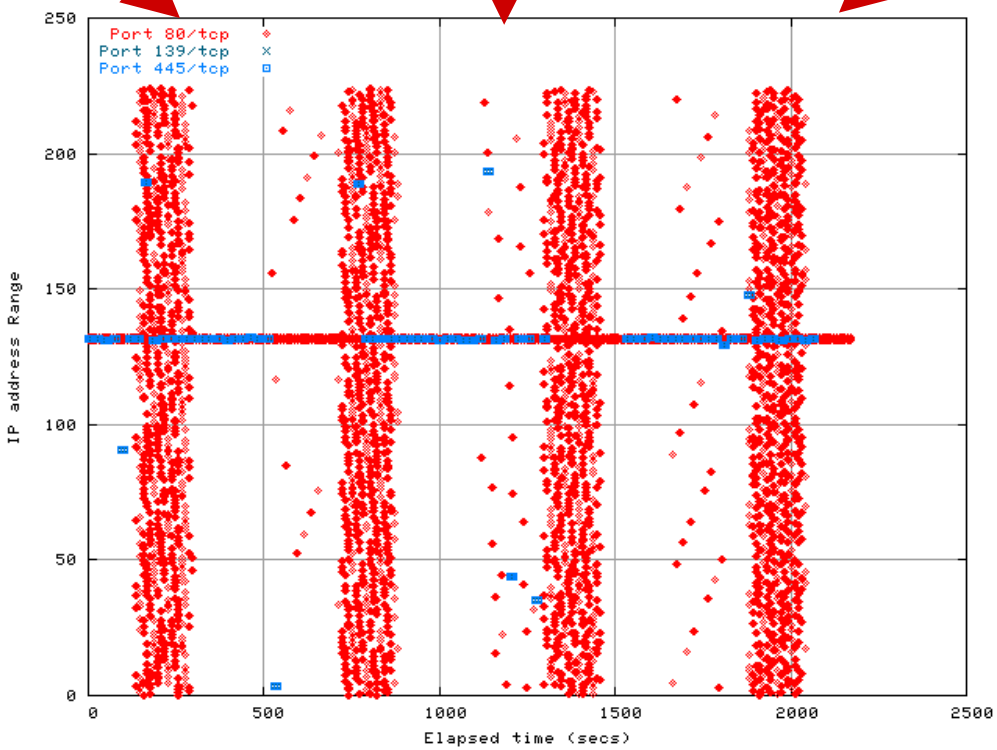


139/tcp



445/tcp

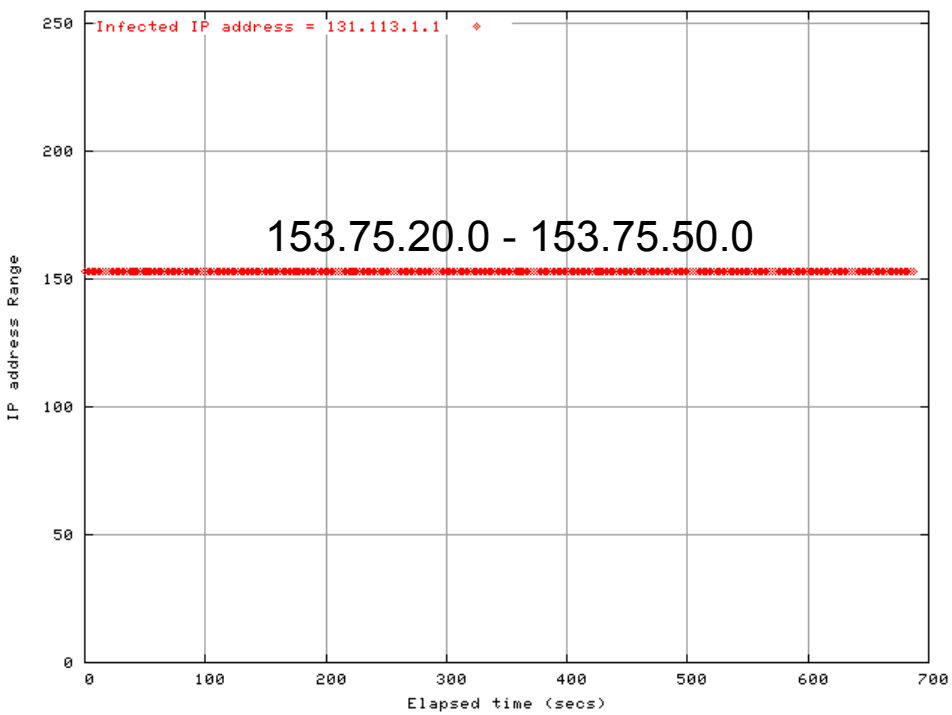


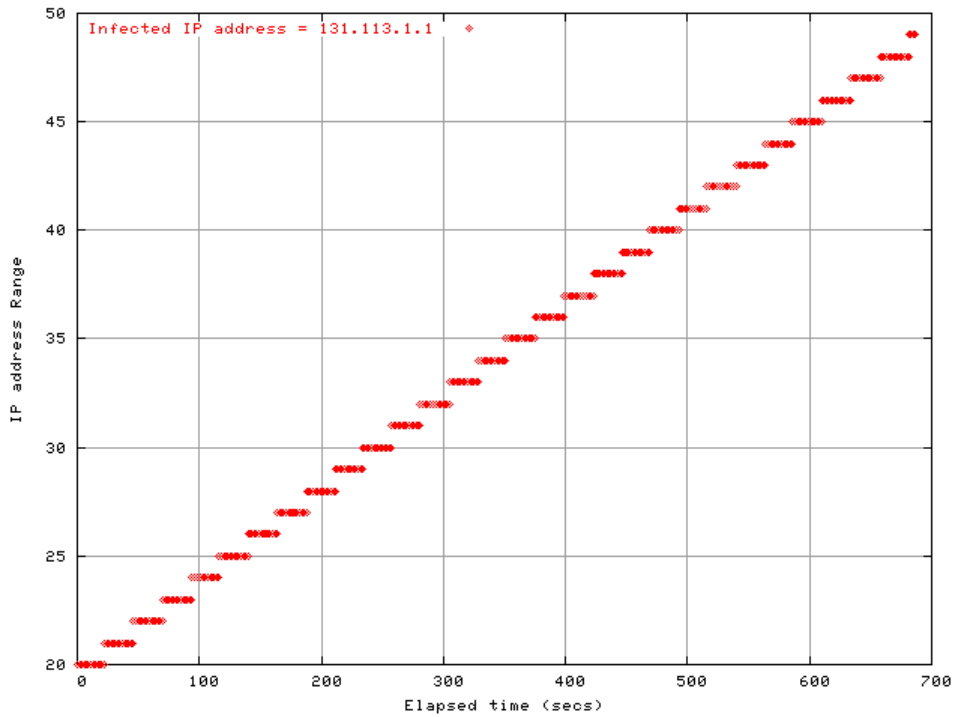


Plot above: from the time obs. started to the time # of pkts reached 51,261.

Retrieval behavior
= Blaster (135/tcp) =

- Blaster selects the start IP address:
  - A completely random IP address with the last octet set to 0 ([1-254].[0-253].[0-253].0) : 60%
  - The first address of its "Class C"-size subnet (x.x.x.0) : 40%
- From there Blaster attempts to infect the following IP addresses sequentially

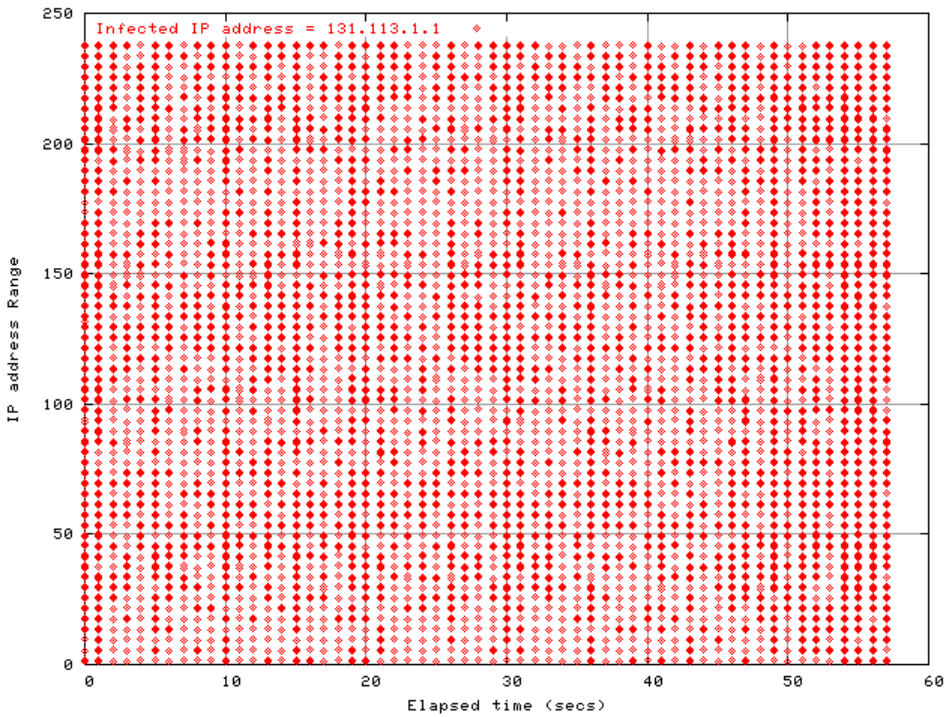


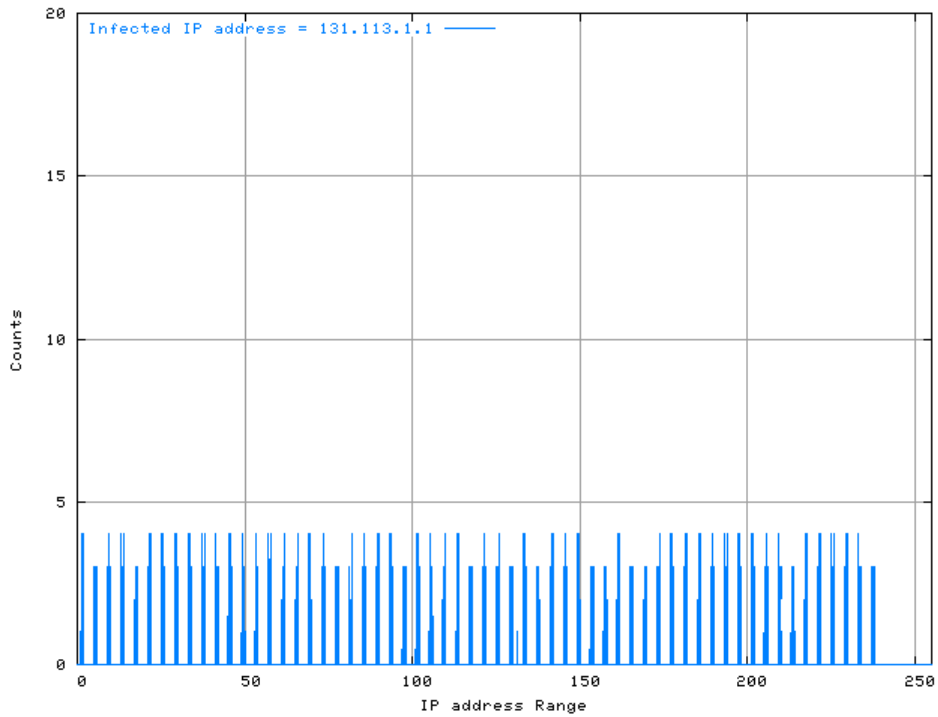


Plot above: from the time obs. started to the time # of pkts reached 7,500 .

Retrieval behavior
= Slammer (1434/udp) =

- Slammer uses the GetTickCount() function of the Win32 API to initialize its random number generator. It uses the random numbers as IP addresses to search for vulnerable hosts.

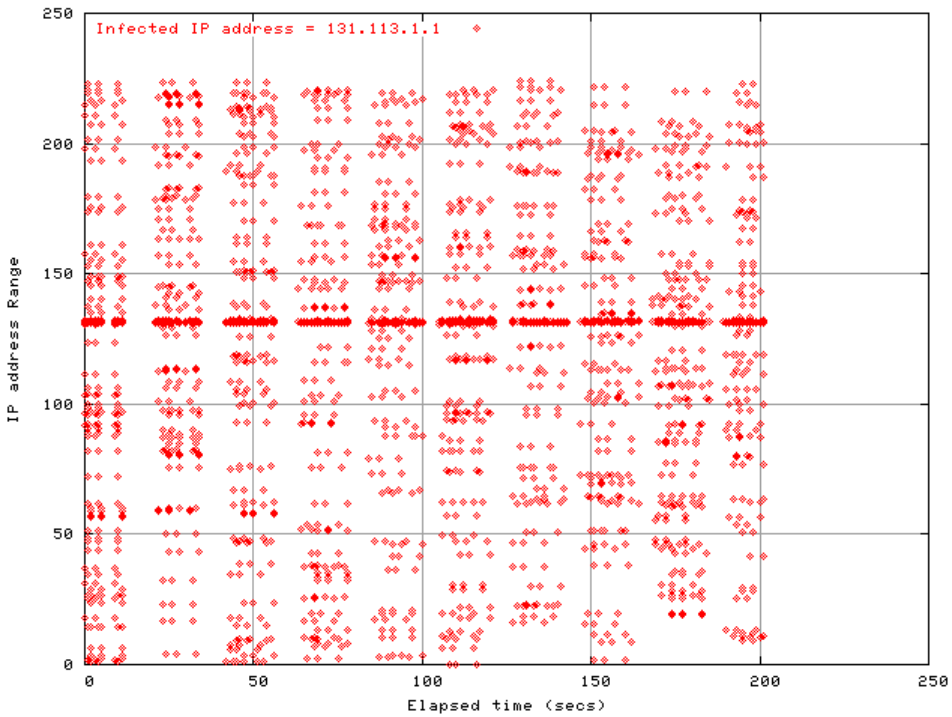


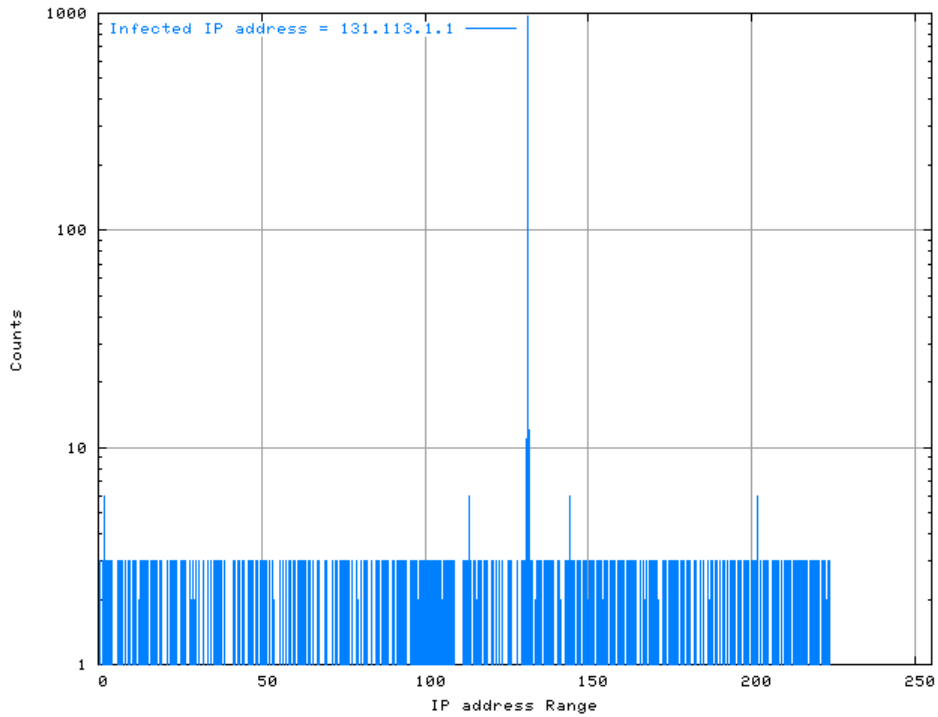


Plot above: from the time obs. started to the time # of pkts reached 10,000.

Retrieval behavior
= Sasser.B (445/tcp) =

Selection of IP address	Experiment Data	Code Analysis
The same first two octets	27.2%	25%
The same first octet	24.6%	23%
Others	48.2%	52%
The average of 5 trials (3,000 packets/trial).		

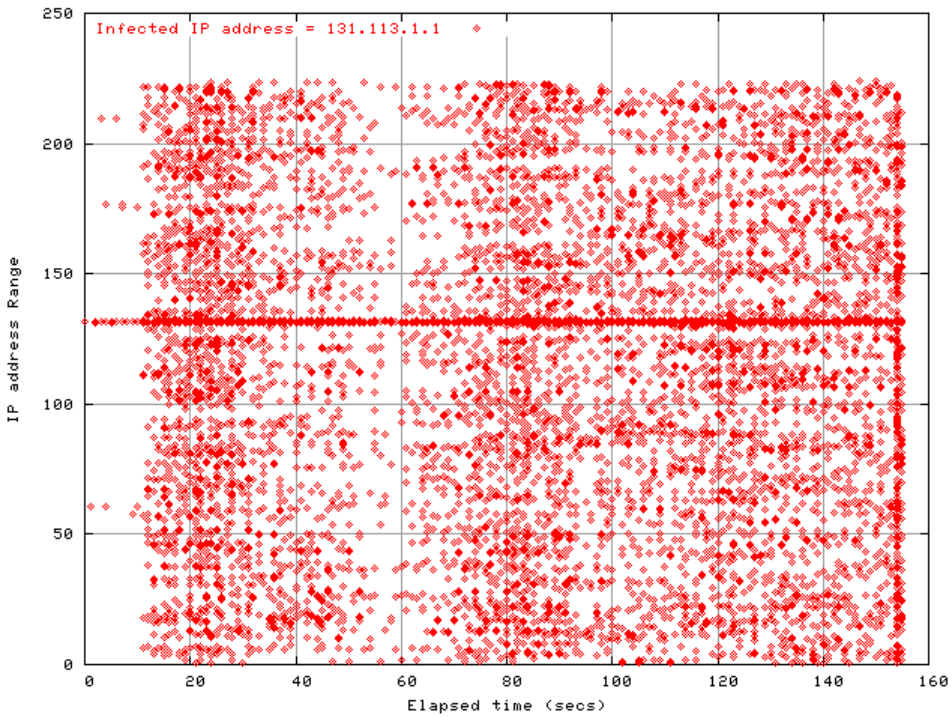


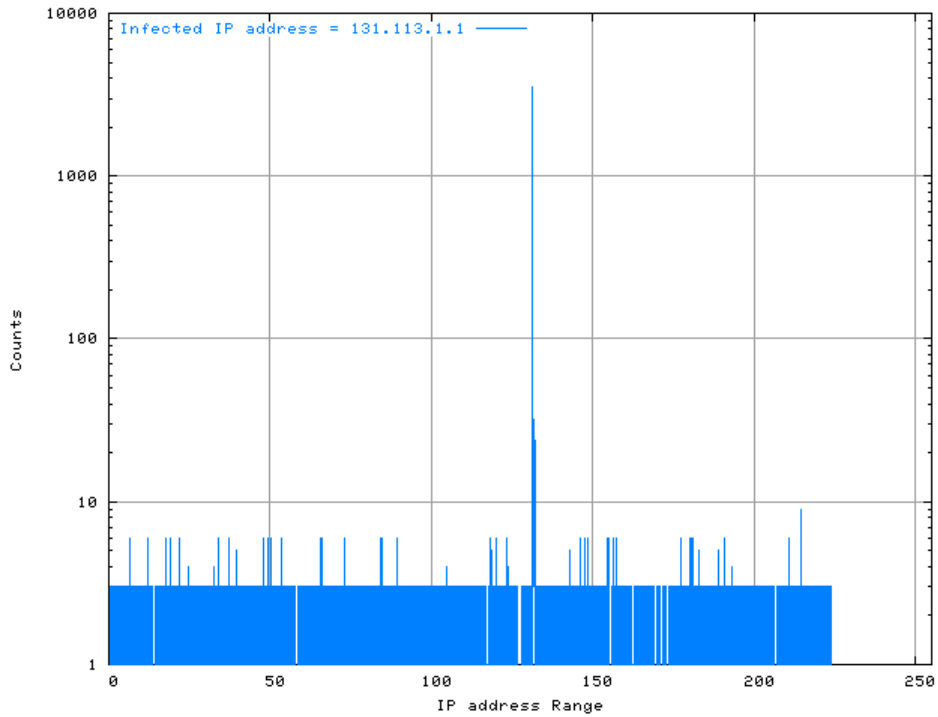


Plot above: from the time obs. started to the time # of pkts reached 3,757.

Retrieval behavior
= Sasser.C (445/tcp) =

Selection of IP address	Experiment Data	Code Analysis
The same first two octets	27.1%	25%
The same first octet	24.8%	23%
Others	48.1%	52%
The average of 5 trials (10,000 packets/trial).		





Plot above: from the time obs. started to the time # of pkts reached 13,602.

Considerations for retrieval behavior of Sasser

- According to the code analysis, completely-random IP address selection accounts for 52%.
  - The same first two octets: a = 52 / (256 * 256) = 0%
  - The same first octet: b = 52 / 256 = 0.2%

- The result of the code analysis shows "a < b".
- The result of the experiment shows "a > b".

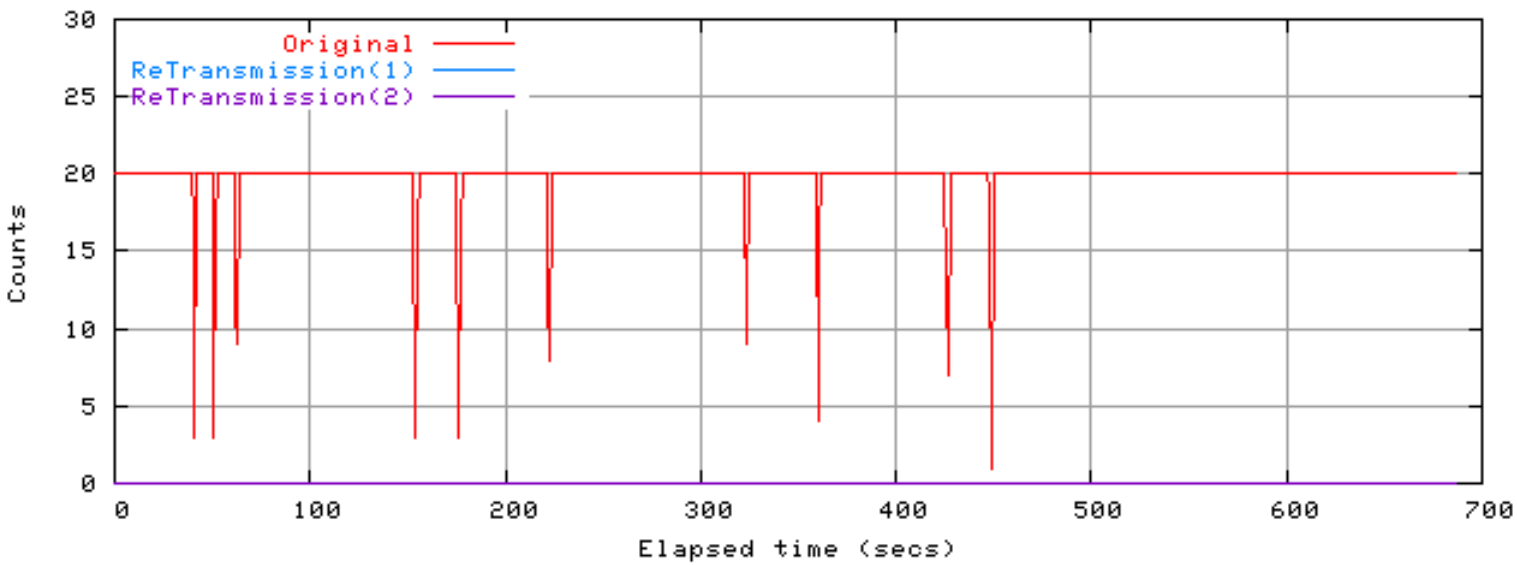
The selection of IP address	Experiment Data	Code Analysis
The same first-two octets	Sasser.B: 27.2% Sasser.C: 27.1%	25% + a
The same first octet	Sasser.B: 24.6% Sasser.C: 24.8%	23% + b
Others	Sasser.B: 48.2% Sasser.C: 48.1%	52% - (a + b)

TCP retransmission behavior = Blaster, Code Red III and Nimda.E =

TCP retransmission is one of the factors which affect infection efficiency.

- Code Red, Nimda, Blaster and Sasser attempt TCP retransmission in the experimental environment as their retrieval behavior.
  - The infected PC sends TCP SYN packets, but it cannot establish a TCP connection because the monitoring PC discards all TCP SYN packets.

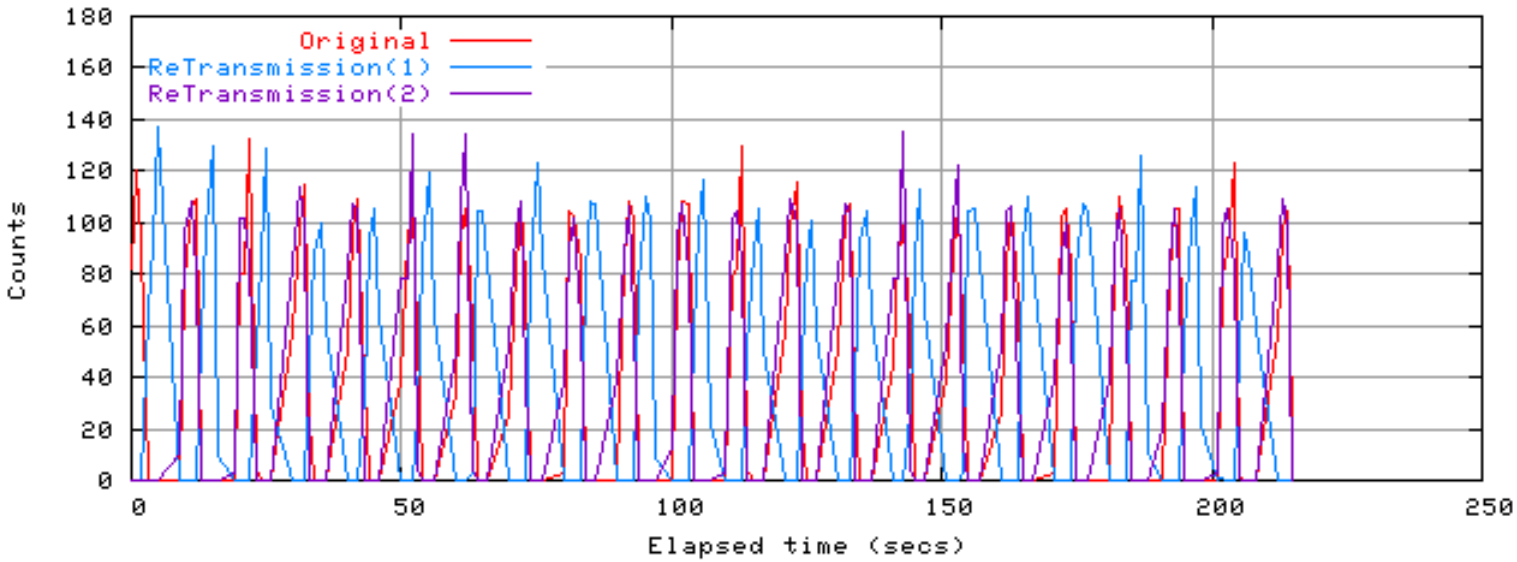
Blaster



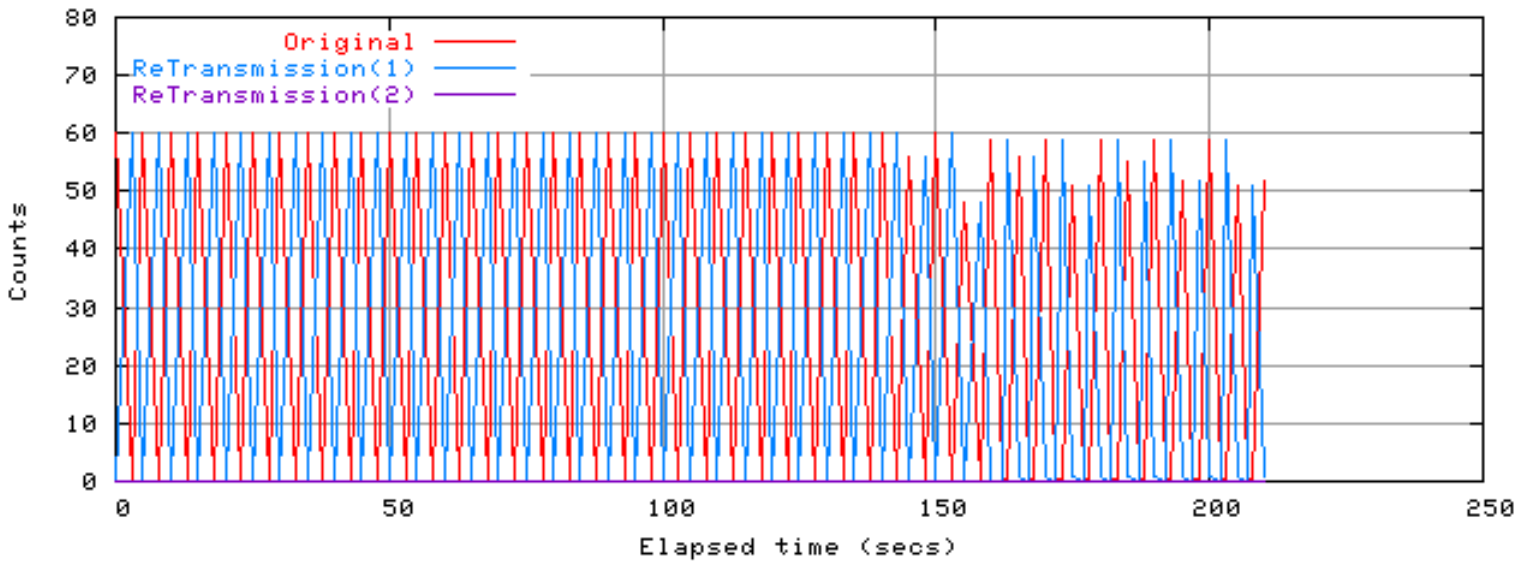
TCP retransmission behavior = Blaster, Code Red III and Nimda.E (cont.)=

Hitachi Incident Response Team

Code Red III



Nimda.E

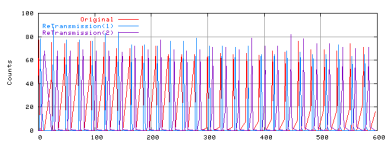
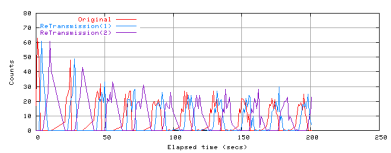
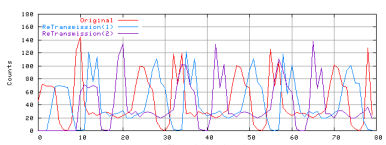
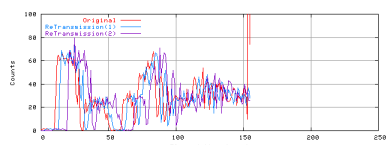


TCP retransmission behavior = Sasser Family=

TCP retransmission is one of the factors which affect infection efficiency.

- According to the code analysis, Sasser infects Japanese Windows XP but does not infect Japanese Windows 2000. What is different in the infection activity of Sasser between Japanese Windows 2000 and Japanese Windows XP?

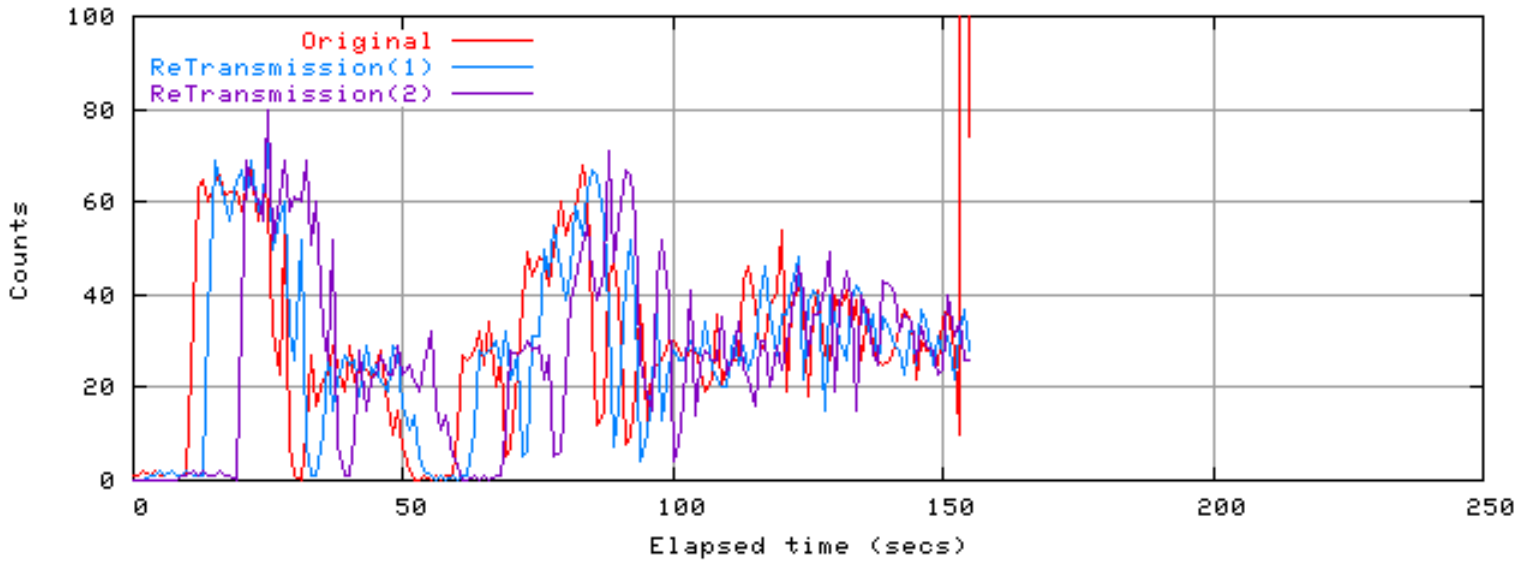
TCP retransmission behavior

	Windows 2000	Windows XP
Sasser.B	**Stable** 	**Little Stable** 
Sasser.C	**Little Stable** 	**Not Stable** 

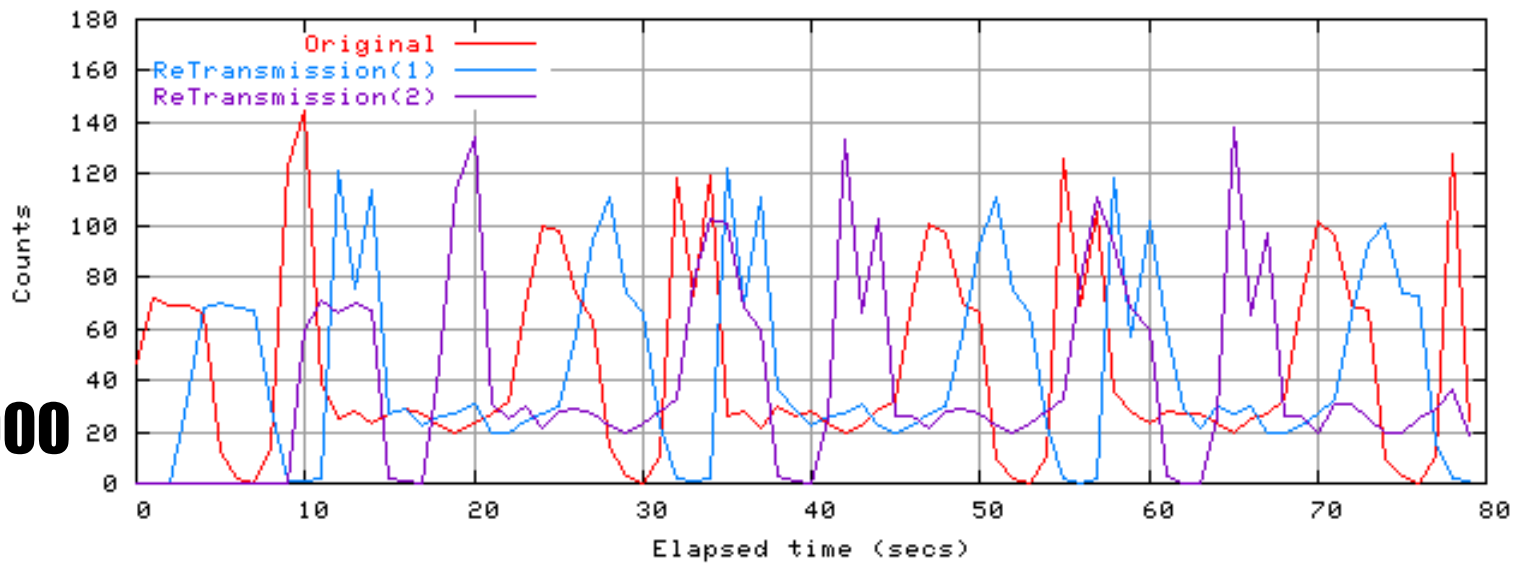
TCP retransmission behavior = Sasser.C =

Hitachi Incident Response Team

Sasser.C Windows XP



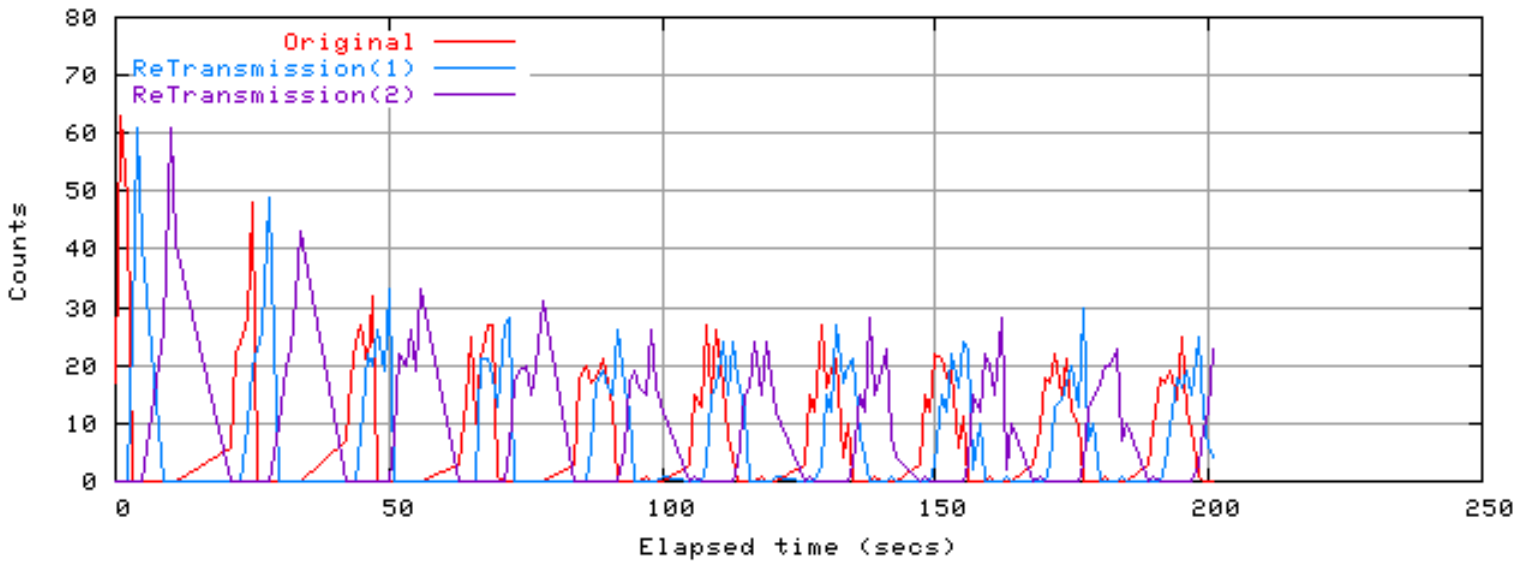
Sasser.C Windows 2000



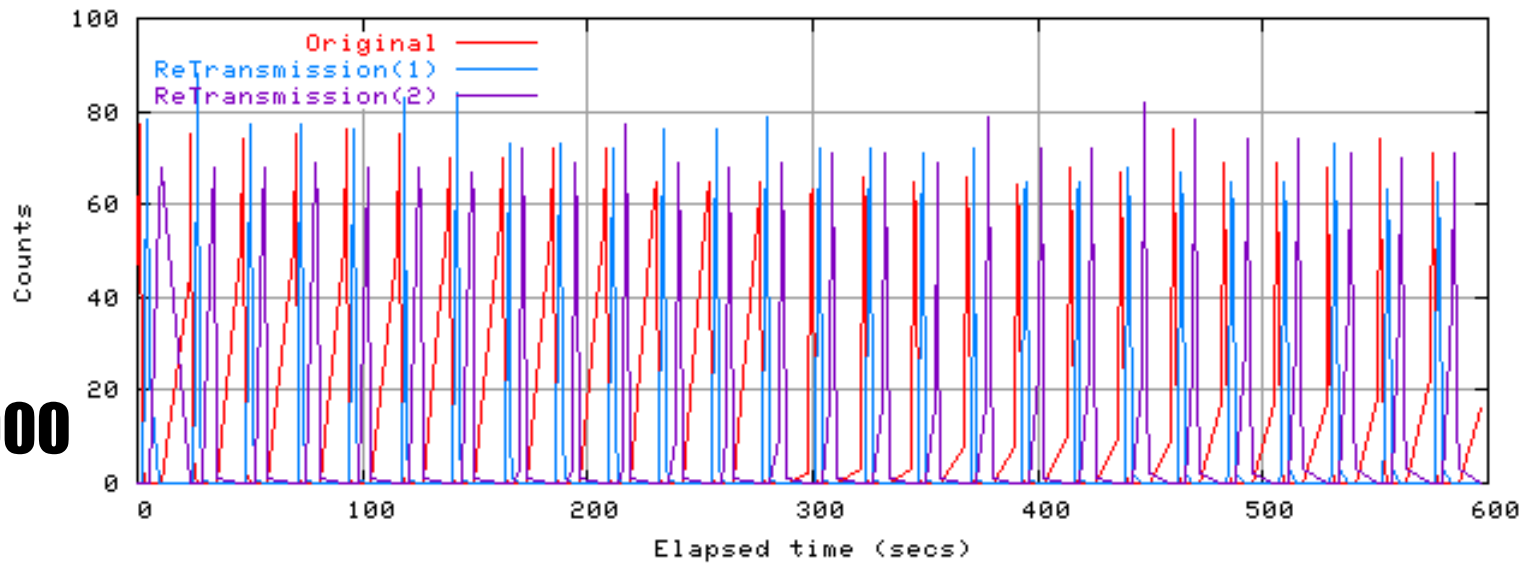
TCP retransmission behavior
= Sasser.B =

Hitachi Incident Response Team

Sasser.B
Windows XP



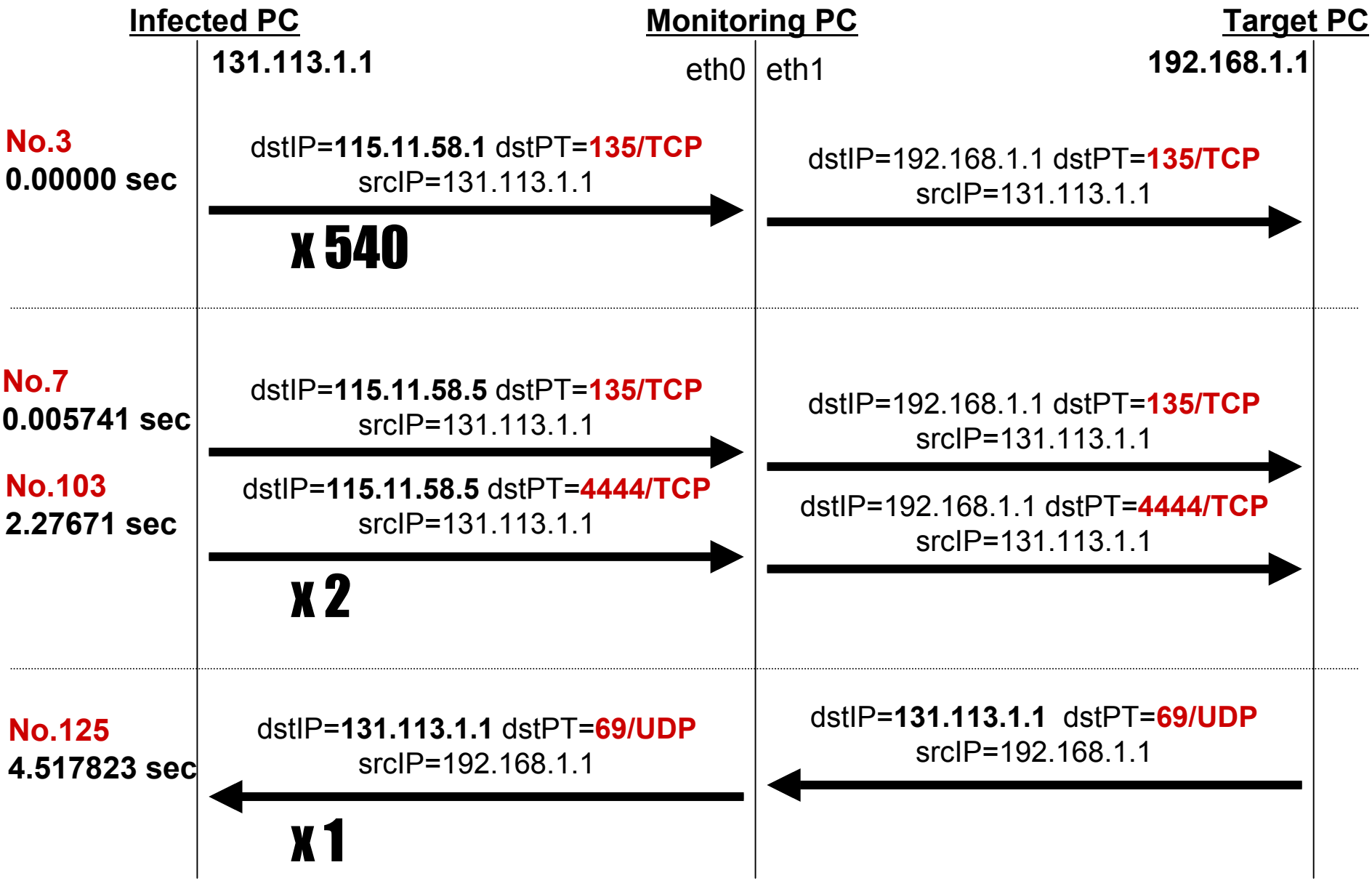
Sasser.B
Windows 2000



Infection behavior = Blaster =

Total packet counts		3,317
Infection activity start time		**3** 0.019219 Packet No, Elapsed Time
The series of port numbers	Counts	The logs of first appearance packet Line1 : **Packet No**, **Elapsed time**, src IP address, dst IP address, Protocol, src PT number, **dst PT number** Line2 : Flag information
135/TCP	540	**3** **0.000000** 131.113.1.1 115.11.58.1 TCP 1032 > **135** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
135/TCP 4444/TCP	2	**7** **0.005741** 131.113.1.1 115.11.58.5 TCP 1036 > **135** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 **103** **2.276719** 131.113.1.1 115.11.58.5 TCP 1052 > **4444** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
69/UDP	1	**125** **4.517823** 192.168.1.1 131.113.1.1 UDP Source port: 1031 Destination port: **69**

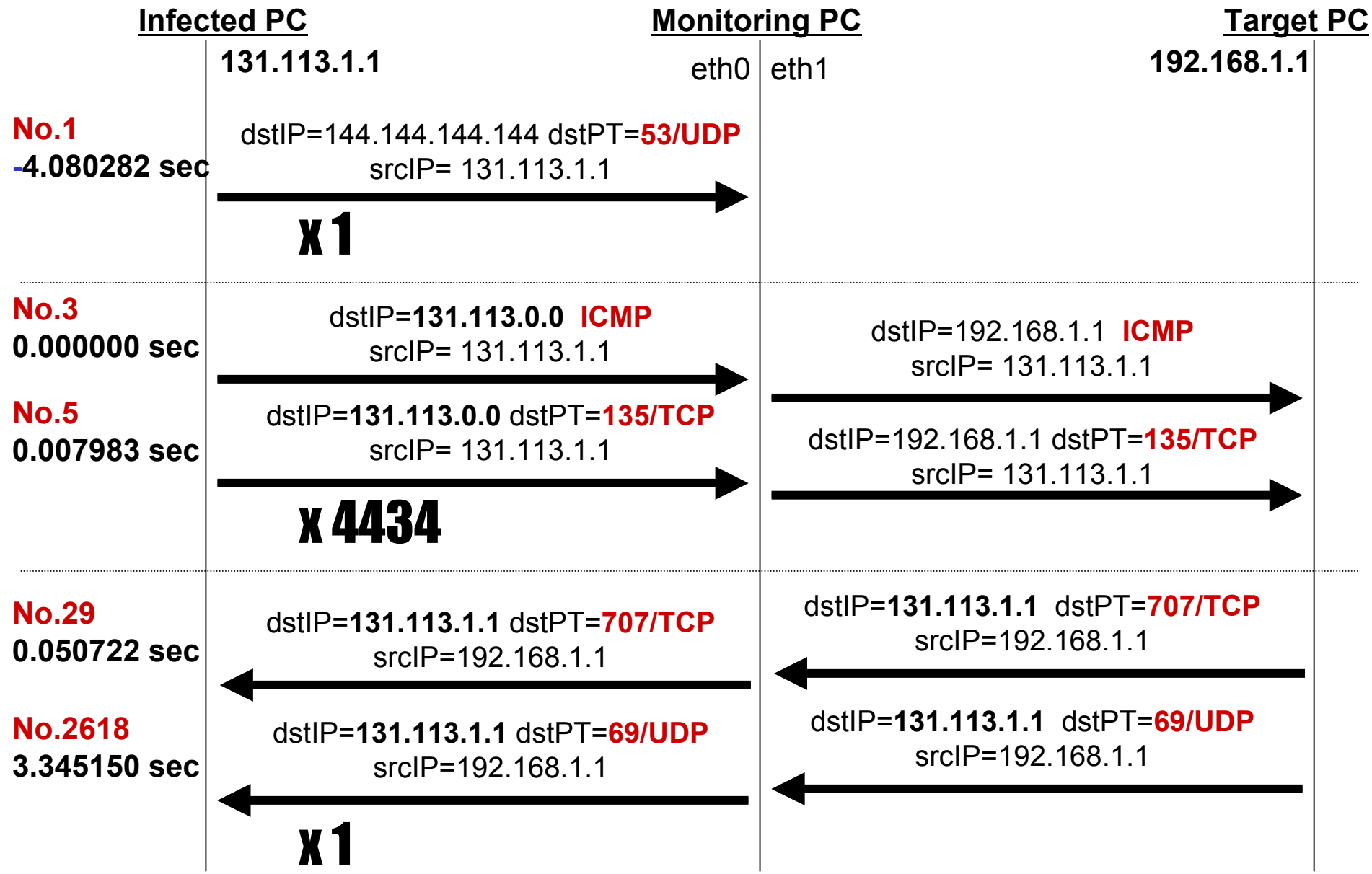
Infection behavior = Blaster (cont.)=



Infection behavior
= Welchia =

Total packet counts		77,448
Infection activity start time		**3** 4.080282 Packet No, Elapsed Time
The series of port numbers	Counts	The logs of first appearance packet Line1 : **Packet No**, **Elapsed time**, src IP address, dst IP address, Protocol, src PT number, **dst PT number** Line2 : Flag information
53/UDP	1	**1** **-4.080282** 131.113.1.1 144.144.144.144 UDP Source port: 1031 Destination port: **53**
ICMP 135/TCP	4434	**3** **0.000000** 131.113.1.1 131.113.0.0 ICMP Echo (ping) request **5** **0.007983** 131.113.1.1 131.113.0.0 TCP 1032 > **135** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
707/TCP 69/UDP	1	**29** **0.050722** 192.168.1.1 131.113.1.1 TCP 3011 > **707** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 **2618** **3.345150** 192.168.1.1 131.113.1.1 UDP Source port: 3060 Destination port: **69**

Infection behavior = Welchia (cont.) =



Build the customized experimental environment to trace the infection behavior of Welchia

Forwarding to DNS server

ipatables -t nat -A PREROUTING
-d 144.144.144.144/32 -i eth0 -j DNAT
--to 131.113.1.2

Packet No.1

dstIP=**144.144.144.144** dstPT=53/UDP

Others (forwarding to Target PC)

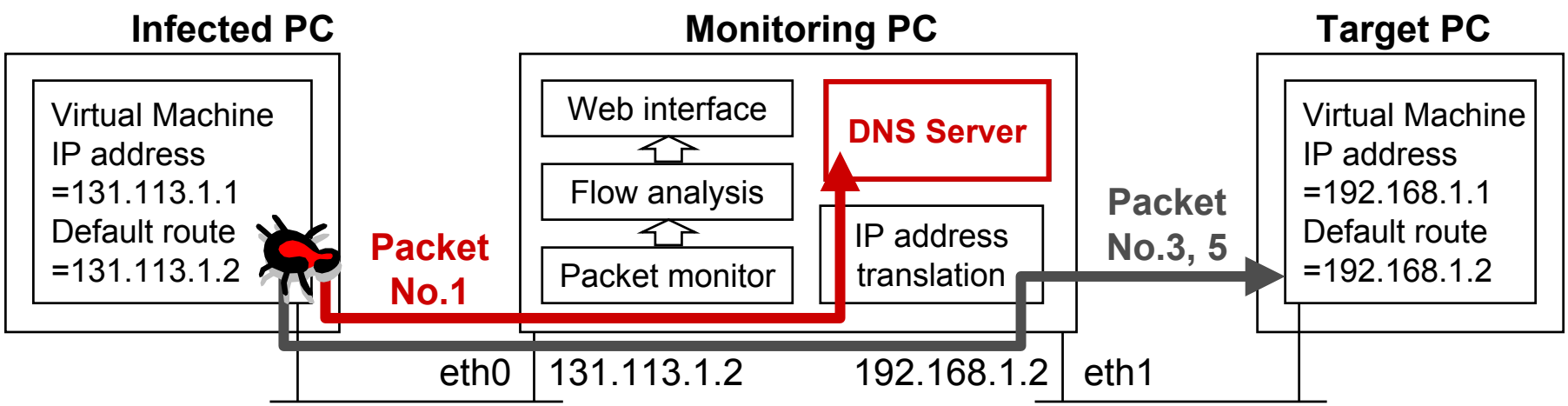
ipatables -t nat -A PREROUTING
-d 0/0 -i eth0 -j DNAT
--to 192.168.1.1

Packet No.3

dstIP=**131.113.0.0** ICMP

Packet No.5

dstIP=**131.113.0.0** dstPT=135/TCP

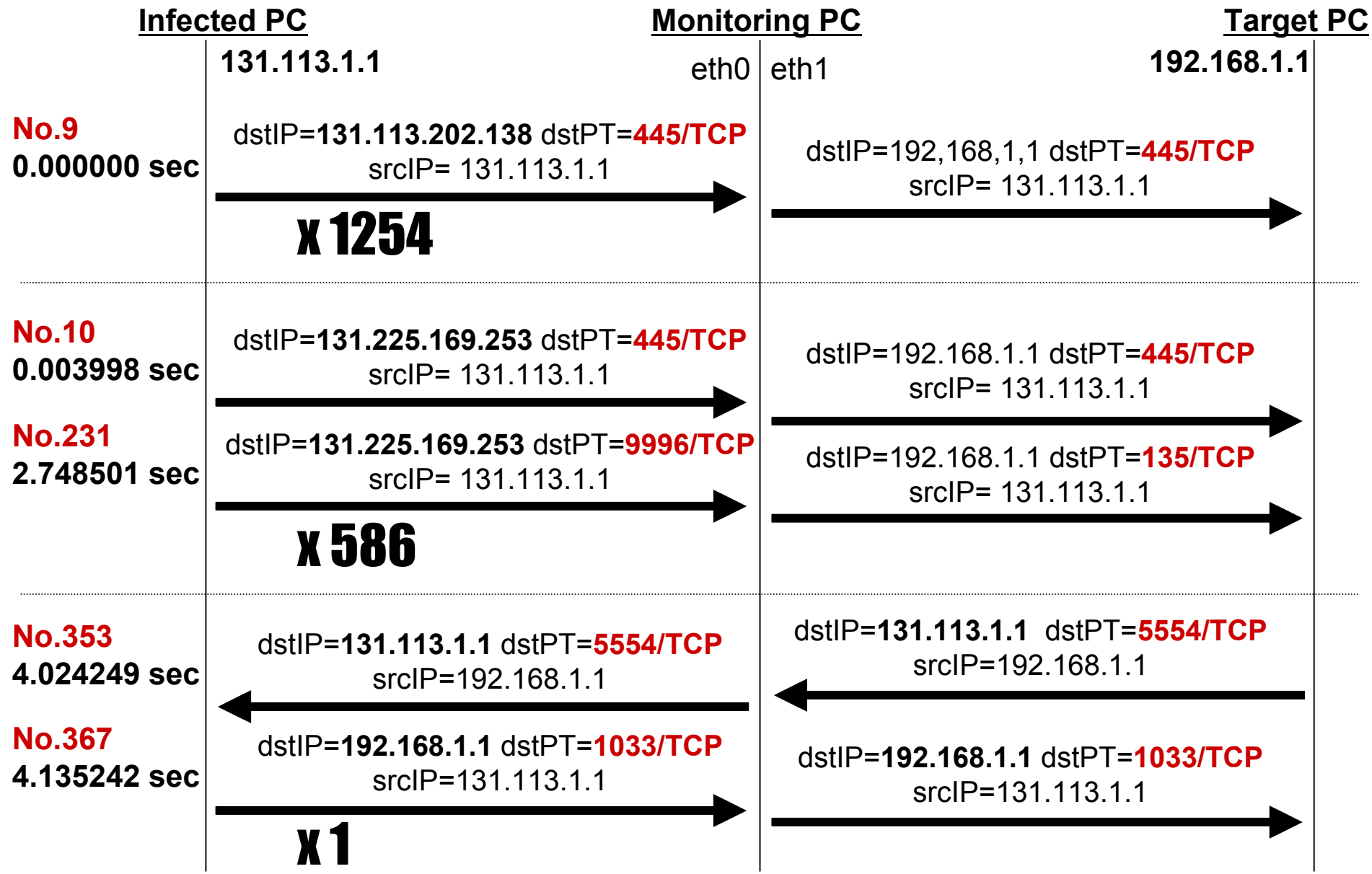


Infection behavior
= Sasser.B =

Hitachi Incident Response Team

Total packet counts		44,509
Infection activity start time		**9** 35.649504 Packet No, Elapsed Time
The series of port numbers	Counts	The logs of first appearance packet Line1 : **Packet No**, **Elapsed time**, src IP address, dst IP address, Protocol, src PT number, **dst PT number** Line2 : Flag information
445/TCP	1254	**9** **0.000000** 131.113.1.1 131.113.202.138 TCP 1054 > **445** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
445/TCP 9996/TCP	586	**10** **0.003998** 131.113.1.1 131.225.169.253 TCP 1055 > **445** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 **231** **2.748501** 131.113.1.1 131.225.169.253 TCP 1075 > **9996** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460
5554/TCP 1033/TCP	1	**353** **4.024249** 192.168.1.1 131.113.1.1 TCP 1032 > **5554** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460 **367** **4.135242** 131.113.1.1 192.168.1.1 TCP 1084 > **1033** [SYN] Seq=0 Ack=0 Win=16384 Len=0 MSS=1460

Infection behavior = Sasser.B (cont.)=



Hitachi Incident Response Team

We have presented:

- Two types of experimental environment
  - For retrieval behavior
  - For infection behavior
- The results of well-known network worms verified in the experimental environments
  - Retrieval behavior
  - TCP retransmission behavior
  - Infection behavior

Our future plans:

- Enhance peripheral functions such as DNS server etc.

  … Build the Tiny, Virtual and Experimental Internet
- Develop experimental environment for advanced malware that detects “non-real” environment thus cannot be invoked on the virtual machine.

Ending

We proposed two types of experimental environment --
"The experimental environment for retrieval behavior"
and
"The experimental environment for infection behavior"
to achieve our objectives.

We described the retrieval behavior of Code Red, Nimda, Slammer, Blaster and Sasser verified in the experimental environments. Also, we described the infection behavior of Blaster, Welchia and Sasser.

uVALUE

THANK YOU

Proposal for the experimental environment
for Network Worm infection

2005/06/29

Masato Terada
Graduate School of Science and Technology, Keio University
Hitachi Incident Response Team, Hitachi Ltd.

HITACHI
Inspire the Next