Broadband Network Virus Detection System Based on Bypass Monitor

Wu Bing[*a], *Yun Xiaochun*[*a], *Xiao Xinguang*[**b]
[a]Research Center of Computer Network and Information Security Technology,
Harbin Institute of Technology
[b]Antiy Labs

ABSTRACT

Network virus are always detected in serial device such as router and firewall generally, limited to the performance of device, the effect virus impose on Internet cannot be detected accurately. To resolve this problem, we have developed a Virus Detection System (VDS) based on bypass monitor that can work on GE level network. With VDS, the virus can be detected in package or data stream according to four methods like binary, URL, E-mail, script. The statistical information of the virus including the virus name, source IP, target IP, spread times and the traffic are provided accurately and presented in charts.

Keywords：VDS，virus，detection

1. INTRODUCATION

The security is one of the biggest challenges facing the Internet. Internet worm appears increasingly since 2000. Especially at 2003, large-scale worm spread all over the world, which had made serious damages. It can be foreseen that such erupt of worm will bring tremendous threat for Internet much more. Internet is an open, complex and huge system [1] in that catastrophe maybe occurs at some certain conditions. It can be seen from worm called Red code[2], Nimda[3], Blaster and Sasser that the damages become more and more heavily with the speed that the computers suffered by worm. As a security accident, erupt of worm makes twice as much, which submits to Moore's Law [4] and Metcalfe Law. [5] Metcalfe's Law states that the usefulness, or utility, of a network equals the square of the number of users. As an open and complex huge system, accident of safety in Internet will occur unavoidably. Therefore supervisory on worm and measurement of flow caused by worm are necessary methodological technique for the normal operation.

2. WORM PROPAGATION

Propagation Characteristic of Worm
As a type of malcode, worm makes a difference from classical virus; it acts as active propagation by network, not by classical physical vector such as floppy disk; Its propagation procedure is to copy a self file to file system or memory, and not attach itself to the executable program.

Propagation Procedure of Worm
First, the worm must copy itself to target system entirely; second, must execute in target system; last, must accompany with other action such as scan and attack for the aim of propagation.

Propagation Way of Worm
There are two different way to spread worm mainly, one is based on regular file transmission protocol, worm copies itself with regular protocol such as SMTP, FTP, and NETBIOS etc. the other way is based on vulnerability，it realize send to target system by buffer overflow. It should be noted that some worm completes its send once basing on vulnerability such Red Code, while some spread after overflow and start of regular file transmission protocol such as Sasser.

Execution in Target System
Worm execution in target system has three modes: First mode is active mode, worm executes itself by remote exploit or other ways and operates in the target, while users are not required to active it. Second mode is Semi-active mode, worm executes itself by remote exploit or other ways in target host with some triggering action but without associated operations by users. Last mode is passive mode: worm should be operated by users, and then can be executed in target host. Therefore such a procedure can be concluded and distinguished from classical virus by the followed Table 1.

Table 1. The difference between worm and virus

	Self copy	Execution	Examples
I-Worm	Active Mode	Passive mode	I-Worm.Netsky
I-Worm Using Previewing vulnerability	Active Mode	Semi-active mode	I-Worm.Nimda
Scan worm	Active Mode	Passive mode	CodeRed, Sasser
Classical Virus	Passive mode	Passive mode	Win95.CIH

Shown by Table 1, the biggest difference between classical virus and worm is that the procedure of network copy is active action. Pressure and effect on the network can be evaluated by measurement since worm spreads actively using network. Pressure and impact on Internet can be evaluated by measurement as Worm can spread actively. A VDS (virus detection system) is designed to evaluate the impact on Internet. In order to inherit custom anti-virus corporation named virus, we called worm as virus as before.

3. REALIZATION OF VIRUS DETECTION SYSTEM

A detection platform for network worm is realized by virus detection system which is based on bypass monitor and combined with high speed rules matched. The structure of systems is shown in Figure 1.

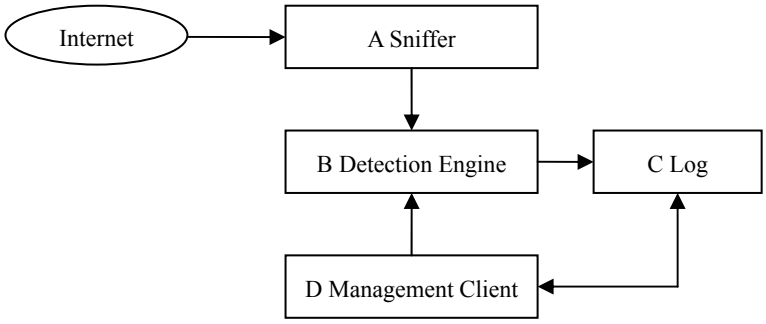

Figure 1 Architecture of virus detection system

The overall design process is: Network gateway data are mirrored to the given port of Ethernet switch， and are supplied to the virus detector engine. The engine monitors the data flow passing the net in a real time. A warning is given immediately, once accessing of sensitive service that is used by worm frequently, or events that are submitted some character mode, are detected. Detail logs are recorded for auditing and tracing afterwards. By this method, virus quadruple information can be recorded effectively that worm use network actions vulnerability, and relative virus and detail evidence for attack can be provided. Such a method supplies a decision supporting for security measure adopted further.

System segments include:

(1) Capture transmission package
(2) Worm scanned for network transmission package (or stream)
(3) Log statistic
(4) System management

Module A is a sniffer engine in Figure 1, which is applied to capture the network and transfer them to the worm detector engine. Using by zero-copy and parallel protocol, the engine increase the speed of package capture. Module B is a virus detector engine, which act as the kernel of the system. The key point of system is to assure efficiency and accuracy of detection because the system is running on backbone network. To detect virus and worm, the traditional method is reassemble content of protocol (e.g. HTTP, SMTP, POP3 and IMAP) to file, which is detected by traditional file virus engine after that. Facing to large traffic, efficiency of detection suffers catastrophic effect. Without reassembling from segment to file, the engine of pressure measurement system detects in packages or stream level directly. A normalized model is adopted by such an engine for optimizing efficiency. Namely, detection for network date is divided into four styles, and four independent detection engines are formed, as shown in Table 2.

Table 2 Four Detection Engines

Match Model	Engine	Worm Style	examples
Original Match	Basic Engine	Scan worm	Sasser
Insensitive Capital Match	URL Engine	WEB scan worm	CodeRed
No Pre-processing Match	Mail Engine	I-worm	I-Worm, Nimda, I-Worm. Netsky
Weighted Match	Script Engine	Script worm	I-Worm, Happytime

Files of knowledge database are formed accordingly, namely character database of primary virus, I-worm, script virus and URL vulnerability. These characters can be divided into:

(1) Transmission characteristic: be extracted match ruler based on stream or packages when worm body is transferred;

(2) Scan characteristic: be extracted based on scanning packages of worm;

(3) Attack (exploit) characteristic: be extracted based on shellcode used by worm or other attack packages.

By means of cooperation with package network sniffer module and detection module, original data are obtained as follows:

(1) I-worm: name, transmission direction, corresponding IP quadruple, application protocol, accumulative transmission times per time unit, transmission traffic of single worm.

(2) Scan worm: category or name, transmission direction, corresponding IP quadruple, application protocol, accumulative scan times per time unit, size of single scan package.

These data will be input to the results pre-processor module and be mined according by flow diagram in Figure 2.

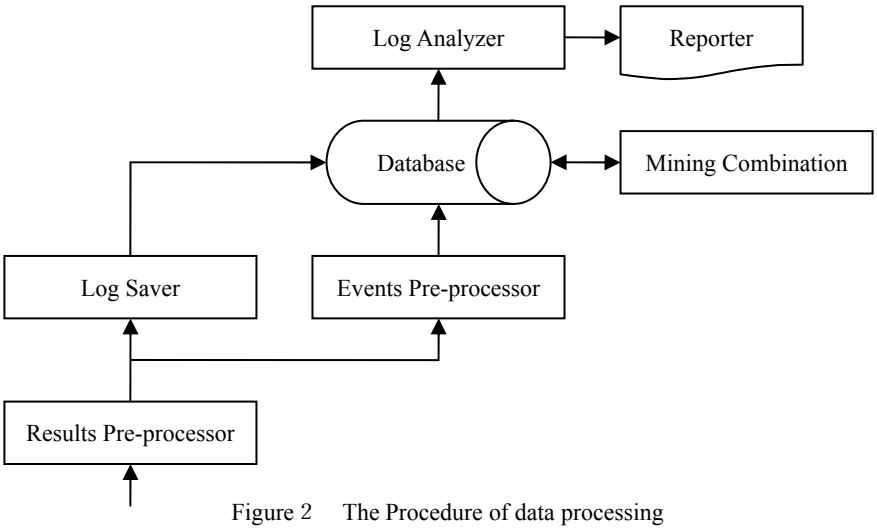

Figure 2 The Procedure of data processing

5. CONCLUSIONS

The VDS is available to detect all kinds of malcode in the nowadays network. The first realized instance of VDS system is running at the network entrance of HIT to protect whole campus network. With the progress of network technology, more and more serious damages may be brought to bear the computer. The most important future work is to add strongly network response to reduce the losing of users.

REFERENCES

[1] Wang Bai-ling,Fang Bin-xing,Yun Xiao-chun,The Distributed Broadband Network Virus Precaution System (In Chinese),Journal of China Institute of Communications,2003,Vol.24 No.8, p.225-230

[2] Changchun Z., Gong Z., Gong W., Towsley D.. Code Red Worm Propagation Modeling and Analysis. Proceedings of the 9th ACM conference on Computer and communications security, ACM Press, 2002: 138-147

[3] Steve R. White. Open Problems in Computer Virus Research. Virus Bulletin Conference, Munich, Germany, October 1999: 22-23

[4] Faloutsos, M., Faloutsos, P. & Faloutsos, C. On power-law relationships of the Internet topology. ACM

SIGCOMM ’99. Computer. Commune. Rev. 1999, 29: 251–263
[5] S. Staniford, V. Paxson, and N. Weaver, How to Own the Internet in Your Spare Time, Proc. of the 11th USENIX Security Symposium, 2002

Contact: Wu Bing, e-mail: wubing@hit.edu.cn; phone: +86 451 86413783 fax: +86 451 86413331 Address: P.B. 320 No.92 Xi Da Zhi St. Harbin, HLJ, P.R.China 150006