原著論文

Workaround for Welchia and Sasser Internet Worms in Kumamoto University

Yasuo Musashi, Kenichi Sugitani,† and Ryuichi Matsuba,†

Center for Multimedia and Information Technologies, Kumamoto University,
Kumamoto 860-8555 Japan,
E-mail: musashi@cc.kumamoto-u.ac.jp,
†*E-mail: sugitani@cc.kumamoto-u.ac.jp,*
†*E-mail: matsuba@cc.kumamoto-u.ac.jp*

Toshiyuki Moriyama‡
Department of Civil Engineering, Faculty of Engineering, Sojo University,
Ikeda, Kumamoto 860-0081 Japan,
‡*E-mail: moriyama@civil.ac*

Abstract: The syslog messages of the iplog-2.2.3 packet capture in the DNS servers in Kumamoto University were statistically investigated when receiving abnormal TCP packets from PC terminals infected with internet worms like W32/Welchia and/or W32/Sasser.D worms. The interesting results are obtained: (1) Initially, the W32/Welchia worm-infected PC terminals for learners (920 PCs) considerably accelerates the total W32/Welchia infection. (2) We can suppress quickly the W32/Sasser.D infection in our university when filtering the access between total and the PC terminal's LAN segments. Therefore, infection of internet worm in the PC terminals for learners should be taken into consideration to suppress quickly the infection.

Keywords: Welchia, Sasser, internet worm, system vulnerability, TCP port 135, TCP port 445, worm detection

1. Introduction

Recent internet worms (IW) are mainly categorized into two types, as follows: one is a mass-mailing-worm (MMW) which transfers itself by attachment files of the E-mail and the other is a system-vulnerability-attack-worm (SVAW) that transfers itself by attack on vulnerabilities of remote buffer overflow in the operating systems and/or the application softwares. The latter SVAW, especially W32/Welchia, its speed is too much fast to fix it, for instance, persons try to re-install the operating system with executing update/fixation program or patch, however, the SVAW like W32/Welchia worm infection has already finished before the re-installation and/or the execution of fixation program. From this point, it is of considerable importance to detect an IP address of the SVAW-infected PC terminal.

One of the attractive solutions to detect of the SVAW is to employ an intrusion detection system (IDS)[1-10]. We know two types of IDSs: One is Snort[10], a rule-based network based IDS, which has a lot of functions such as packet capture, IP defragmentation, TCP stream reassembling (stateless/stateful), and content matcher (detection engine). The other is iplog[11], a packet logger that is not so powerful as Snort but it is slim and light-weighted so that it is useful to get an IP address of the client PC terminal.

In July 16th, 2003, Widows Update of MS03-26 (Vulnerability of Windows RPC) has been released and after for a while, many Windows PC terminals are worldwidely infected with W32/Blaster and/or W32/Welchia SVAWs. In our university, infection of W32/Blaster is initially blocked by a fire wall (FW) in the barrier segment, however, infection of W32/Welchia is unfortunately kicked and spreaded out widely by the note PCs that are brought carelessly. We installed iplog into our DNS server (**kPlog**) to detect an IP address of W32/Welchia infected PC terminal and automatically inform its detection to a staff who manages the detected IP address.

The present paper is to discuss (1) on correlation between the total traffic of infection of W32/Welchia and the partial traffic of infection from PC terminals for learners, and (2) how to prevent infection of

W32/Sasser.D, as quick as possible.

2. Observations

2.1 Network Systems

We investigated traffic of TCP session access between the top domain DNS server (**kPlog**) † and the PC clients. Figure 1 shows a schematic diagram of a network observed in the present study. **kPlog** is one of the top level domain name (kumamoto-u) system servers and plays an important role of subdomain delegation and domain name resolution services for many PC terminals.

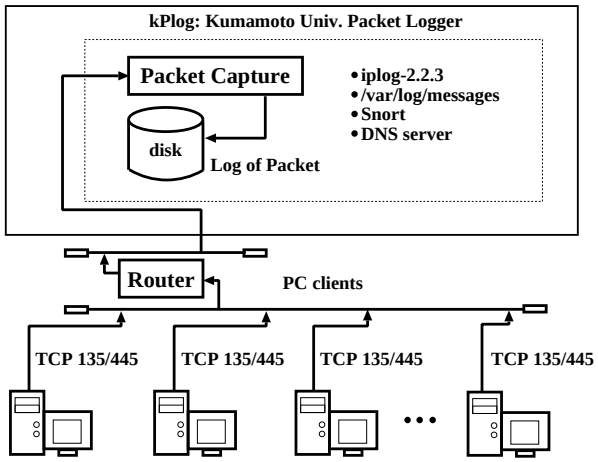

Figure 1. A schematic diagram of a network observed in the present study.

2.2 SVAW Detection System

We designed and developed a new detection system for a SVAW detection system (SDS). This system consists of packet capture for TCP port 135, a detection engine "wscan", and an alert mailer "smail". The procedures for the detection system are properly worked out to a Perl "welwat.pl" script that executes "wscan" in a time per 10 seconds.

In **kPlog**, the iplog-2.2.3 program package has been employed as a syslog message recorder of TCP packets in which syslog messages includes both source IP and TCP port addresses of the client.

The detection engine "mscan" is a C-shell script program consisting of three components, a packet preprocessor, a difference checker, and an alert E-mailer without a local MTA "smail". In an initial step, "mscan" renames the "newdb" file as the "olddb" file. The packet preprocessor is a "grep" command that extracts only a TCP packet with a port of 135 and print out it into the "newdb" file. The difference checker is a "diff" command with an option "-c" to check difference between "olddb" and "newdb" files. After the checker, if the "newdb" file differs from the "olddb" one, and then this difference is printed out to a "mailbody" file. From the file, "mscan" checks the E-mail address list of network managers and e-mails to the network manager by the "smail" program. This program is compiled by the gcc-3.2.3 C compiler.

In the case of W32/Sasser.D, the packet preprocessor is modified to extract only a TCP packet with a port of 445.

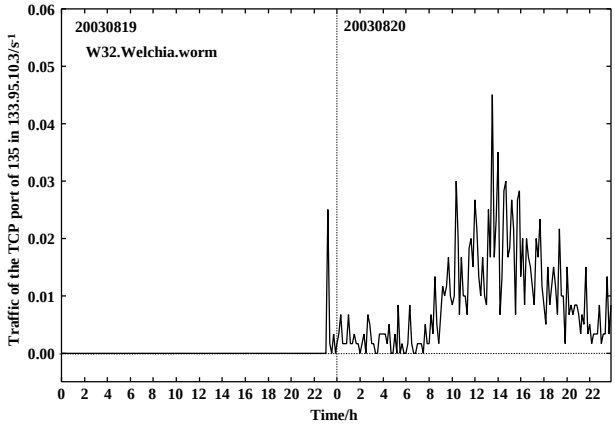

Figure 2. Traffic of the TCP port 135 trial access to the IP address of 133.95.10.3 through August 19th to 20th, 2003 (s^{-1} unit).

2.3 Traffic of the TCP port 135 Access

We observed traffic of TCP port 135 access packets from W32/Welchia system-vulnerability-attack worm (SVAW)-infected PC terminals to the top domain DNS server **kPlog** through August 19th to 20th, 2003, as shown in Figure 2. In our university, **kPlog** is an only DNS server and a Linux system without any Samba related server programs[12] so that it receives usually the UDP packets as a port of 53. However, it starts to receive a plenty of illegal TCP packets as a port of 135 when the W32/Welchia worm-infected PC terminals are increasing.

Although we have already configured the setup of the fire wall in the barrier segment to filter the TCP port of 135 to stop the worm infection attack, unluckily, in Figure 2, the TCP packets has been detected after 23:00, August 19th, 2003. This is because a few

†**kPlog** is a top domain DNS server in Kumamoto University (kumamoto-u). The OS is Linux OS (kernel-2.4.26), and hardware is an Intel Xeon 2.40GHz Dual SMP machine.

of the note PC users had taken the W32/Welchia infected PCs into our LAN and connected it.

3. Results and Discussion

3.1 PC terminals for Learners

We illustrate the observed traffic of the TCP port 135 infection packets between the top domain DNS server (**kPlog**) and the W32/Welchia system-vulnerability-attack worm (SVAW)-infected PC terminals in Figure 3 through August 19th, 2003 to January 31st, 2004. In Figure 3, the total traffic curve of the TCP 135 infection packets is initially similar to that of the TCP 135 infection packets from the PC terminals for learners. However, this similarity gradually decreases and the traffic itself disappeared at last.

This result is interpreted in terms of the following facts: (1) We have 920 PC terminals for learners, which has a large scaled potential for internet worm breeding. These PC terminals have been designed to recover their hard drive disks from their master disk images provided by the file server for recovery when detecting changes in their hard drive disks. (2) Unfortunately, modification of the master disk image is carried out only twice per year. The summer modification was performed through August 21st to September 9th, 2003. In fact, the traffic from PC terminals for learners gradually decreases and the traffic disappeared after September 9th.

After the modification, we started to inform network managers about IP addresses of the SVAW-infected PC terminals, manually. From this work, it is sure that the traffic of TCP 135 infection access drastically decreases at 16th September, 2003. But this TCP 135 infection access never ceases even though it spent 60 days (see Figure 3).

We prepared a fully automated W32/Welchia SVAW detection notification system (SDS) and implemented it into **kPlog** at 21st October, 2003. This system transmits an E-mail to a network manager when detecting W32/Welchia SVAW. After installation this SDS, the traffic of TCP port 135 infection access is suppressed to be under 50-200/day. This is because this system simultaneously transmits as detected IP address of the W32/Welchia-infected PC so that the network manager can do workaround as quick as possible. Finally, the traffic of TCP 135 port infection access is terminated after January 1st, 2004, exceptionally at January 5th, 2004. The detection system is stopped at January 31st, 2004.

As a result, it is clear that (1) a lot of PC terminals

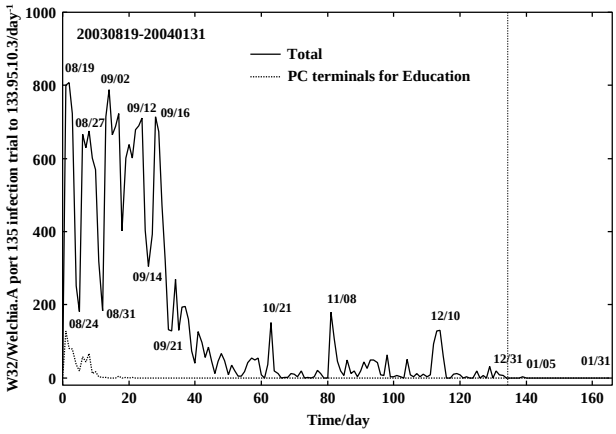

Figure 3. Traffic of the TCP port 135 infection access to the IP address of 133.95.10.3 through August 19th, 2003 to January 31st, 2004 (day^{-1} unit). Both solid and dotted lines show the total traffic and the traffic from PC terminals for education (133.95.3x.0/24), respectively.

for learners considerably contributes to breed a system-vulnerability-attack worm (SVAW), and (2) rapid notification is effective to suppress the traffic of SVAW infection access like W32/Welchia. These informations are very useful for the next W32/Sasser SVAW.

3.2 Infection of W32/Sasser.D

The vulnerability of Local Security Authority Subsystem Service (LSASS), as MS04-11 has been published in April 15th, 2004. This vulnerability includes stack-based buffer overflow in certain functions of Active Directory Service (ADS). We noticed that the ADS uses TCP port 445 to connect RPC service so that a new system-vulnerability attack worm (SVAW) infects Windows PC terminal with itself via this TCP port 445. Therefore, we filter TCP port 445 from/to the university outside. Also, we filter TCP port 445 from/to the LAN segment of PC terminals for learners. We have also implemented the SVAW detection system (SDS) against a new SVAW into **kPlog** in which the SDS is observing TCP port 445.

In May 7th, 2004, the SDS starts to detect the abnormal TCP port 445 access to **kPlog**. After a while, this access is identified as W32/Sasser.D SVAW infection trial access. In the case of the W32/Sasser.D SVAW, we were able to suppress initially increasing of its infection. In fact that traffic of the TCP port 445 is considerably lower than that of the TCP 135 (see Figure 4). At the first stage, 800 IP/day are detected for W32/Welchia, while 400 IP/day are observed for W32/Sasser.D, respectively. The detection of W32/Sasser.D is gradually decreased to May 31st, 2004. Finally, the detection of an IP address of

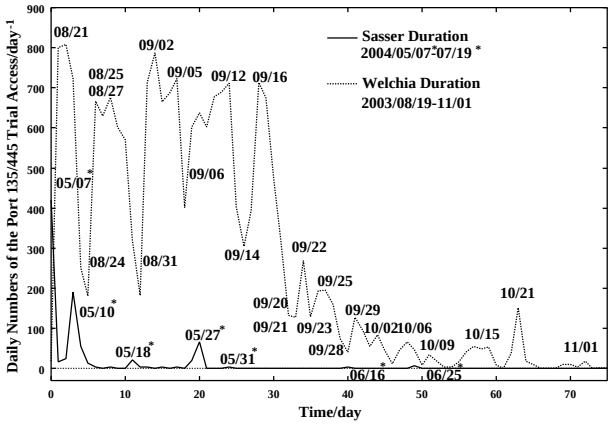

Figure 4. Traffic of the TCP port 445/135 infection access to the IP address of 133.95.10.3 through 75 days (day^{-1} unit). Both solid and dotted lines show traffics of W32/Sasser and W32/Welchia, respectively.

W32/Sasser.D-infected PC terminals has been continued to be zero at the present time.

4. Concluding Remarks

We statistically investigated system log (syslog) files of the iplog-2.2.3 packet capture program daemon in the top DNS server **kPlog** in Kumamoto University when receiving abnormal TCP packets from PC terminals infected with system vulnerability attack worm (SVAW) like W32/Welchia or W32/Sasser.D internet worm. By monitoring the TCP port 135/445 packet access, we have found information about how to suppress initial infection of SVAW: (1) The infection traffic of SVAW like W32/Welchia is significantly contributed by PC terminals for learners (920 PCs). (2) The 920 PC terminals, if they have several system vulnerabilities, are considerable to be a big threat. (3) When taking the threat into consideration, the W32/Sasser.D infection in our university can suppress quickly by only filtering the access between total and the PC terminal's LAN segments. From these results, it can be said that it is important to prevent infection of internet worm in the PC terminals for learners.

We continue further investigation to get more detailed information on the mass mailing worm (MMW)-infection in the PC terminals for learners[13].

Acknowledgement. All the calculations and investigations were carried out in Center for Multimedia and Information Technologies (CMIT), Kumamoto University. We gratefully thank to all the CMIT staffs and system engineers of MQS (Kumamoto) for daily supports and constructive cooperations.

References and Notes

[1] Northcutt, S. and Novak, J., *Network Intrusion Detection*, 2nd ed; New Riders Publishing: Indianapolis (2001).

[2] Yang, W., Fang, B. -X., Liu, B., Zhang, H. -L., Intrusion detection system for high-speed network *Comp. Commun.*, Vol. 27, 2004 in press.

[3] Denning, D. E.: An Intrusion-detection model, *IEEE Trans. Soft. Eng.*, Vol. SE-13, No.2, pp.222-232 (1987).

[4] Laing, B.: How To Guide-Implementing a Network Based Intrusion Detection System, http://www.snort.org/docs/iss-placement.pdf, ISS, 2000.

[5] Mukherjee, B., Todd, L., and Heberlein, K. N.: Network Intrusion Detection, *IEEE Network*, Vol. 8, No.3, pp.26-41 (1994).

[6] Warrender, C., Forrest, S., and Pearlmutter, B.: Detecting Intrusions Using System Calls: Alternative Data Models, *Proc. IEEE Symposium on Security and Privacy*, No.1, pp.133-145 (1999).

[7] Hofmeyr, S. A., Somayaji, A., and Forrest, S.: Intrusion Detection Using Sequences of System Calls, *Computer Security*, Vol. 6, No.1, pp.151-180 (1998).

[8] Ptacek, T. H. and Newsham, T. N.: Insertion, Evasion, and Denial os Service: Eluding Network Detection, January, 1998, http://www.robertgraham.com/mirror/Ptacek-Newsham-Evasion-98.html

[9] Anderson, D., Lunt, T. F., Javitz, H., Tamaru, A., and Valdes, A.: Detecting unusual program behavior using statistical component of the Next-generation Intrusion Detection Expert System (NIDES), *Computer Science Laboratory SRI-CSL-95-06*,1995.

[10] http://www.snort.org/

[11] http://ojnk.sourceforge.net/

[12] http://www.samba.org/

[13] Matsuba, R., Musashi, Y., and Sugitani, K.: Detection of Mass Mailing Worm-infected IP address by Analysis of Syslog for DNS server, *IPSJ SIG Technical Reports, Distributed System and Mangement 32nd*, Vol. 2004, No.37, pp.67-72 (2004).