Journal of Medical Systems, Vol. 26, No. 3, June 2002 (© 2002)

A Filter That Prevents the Spread of Mail-Attachment-Type Trojan Horse Computer Worms

Shinji Kobayashi,[1,4] Masamichi Goudge,[2] Toshio Makie,[1] Eisuke Hanada,[1] Mine Harada,[3] and Yoshiaki Nose[1]

The malicious code "W32/Sircam" is spread via e-mail and potentially through the file space shared by local area networks. Such Trojan-horse-type computer worms easily penetrate Internet firewalls and propagate via the "backdoor" to other computers. Once a malicious code, such as "W32/Sircam," has been executed on a system, it may reveal or delete confidential data, such as clinical records. In order to protect against the leakage of clinical records, we devised a mail filter that successfully prevents the spread of mail containing this malicious code. It is significant that neither access control nor packet filtering is guaranteed to prevent the spread of this mail-attachment-type Trojan horse computer worm.

KEY WORDS: Internet; security issue; clinical record; e-mail; computer worm; filter.

INTRODUCTION

The Internet is a powerful environment for communication and data transaction. Biology and medical science has benefited from the Internet, and new findings and clinical investigation are shared worldwide simultaneously by the Pubmed®, publication database.(1) Various medical applications are available on the Internet, including telemedicine,(2) educational programs,(3) and interhospital data relays.(4)

On the other hand, unscrupulous individuals often attempt to use the Internet to access and steal confidential information, alter web pages or bank deposits, and spread computer viruses. CERT® reported that the number of Internet incidents has increased rapidly recently (Fig. 1).(5)

[1] Department of Medical Information Science, Kyushu University Graduate School of Medical Sciences, Fukuoka 812-8582, Japan.

[2] Kyowakai Medical Corporation, 119-1 Fudokoro, Kanuma, Tochigi 322-0033, Japan.

[3] Medicine and Biosystemic Science, Internal Medicine, Medicine and Surgery, Kyushu University Graduate School of Medical Sciences, Fukuoka 812-8582, Japan.

[4] To whom correspondence should be addressed; e-mail:skoba@intmed1.med.kyushu-u.ac.jp.

0148-5598/02/0600-0221/0 © 2002 Plenum Publishing Corporation

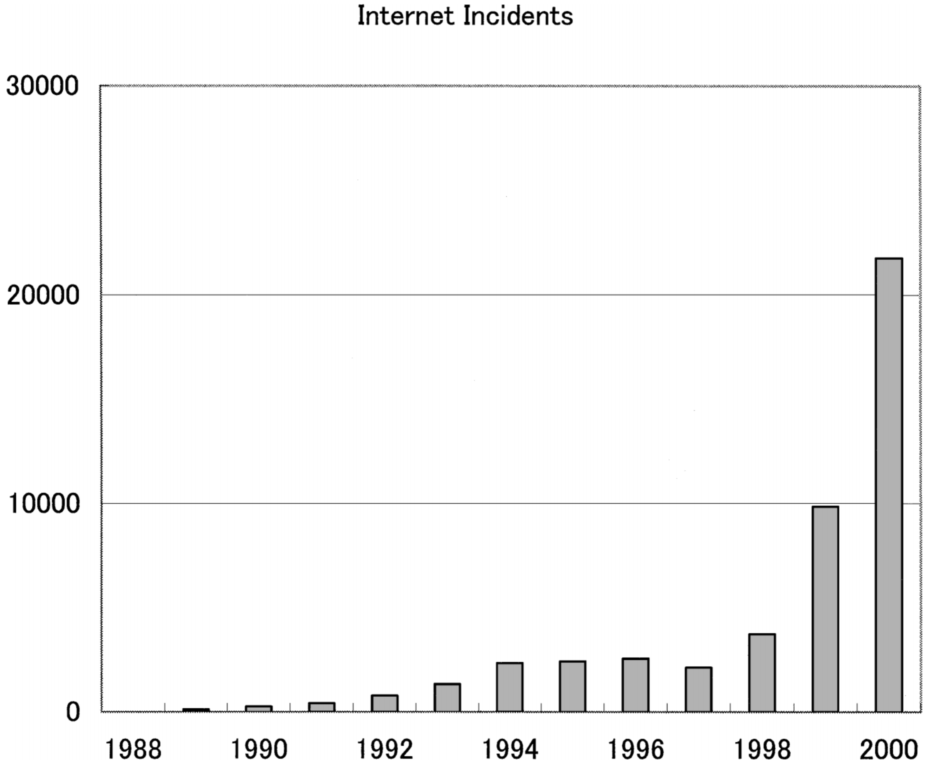


Fig. 1. CERT reported incidents on the Internet.

Some network techniques have been developed to protect against such improper access. Packet filtering is a well-known Internet firewall that checks and controls the port of entry and the passage of packets; it allows only a secure port from the Internet to the intranet, and does not transmit unsecured packets from the intranet to the Internet. Hospital information systems that contain patients' clinical records have to be carefully isolated and protected by firewalls. When clinical records are transmitted between institutions, they usually have to be encrypted to prevent unauthorized access. Virtual private network and virtual LAN technologies are expected solutions to this security issue.(6,7) However, mail-attachment-type Trojan worms, such as "W32/Sircam," easily get past packet filters and can send unencrypted mail to others,(8) because the worm's own SMTP (simple mail transfer protocol) engine uses the normal SMTP port, 25, and other mail transfer agents identify the malicious code as normal mail. Once "W32/Sircam" has been executed on a Microsoft Windows system, it can distribute or delete files in the "My Documents" folder, such as clinical patient records.

To prevent an outbreak of Trojan-horse-type worms, such as "W32/Sircam," and to protect against leaks of medical information, we devised a filter that is used in the mail transfer agent (MTA), which successfully rejects mail contaminated with

"W32/Sircam." This filter system should also be applicable to other malicious codes, such as "W32/Nimda."(9)

METHODS

Mail Server Settings

Our mail server consists of a Compaq Prolinea 4/33cx, an IBM PC/AT compatible machine, which has an i486SX/33 MHz CPU, 12 Mbytes RAM, a 340-Mbyte HDD, and an NE-2000-compatible ethernet interface card. The network software was based on FreeBSD 2.2.8-stable as the operating system, and Postfix 20010228pl3 was installed as the mail transfer agent with the PCRE (Perl Compatible Regular Expression) option. The configuration file was changed to enable the new filter (List 1).

Filter Setup

The filter (List 2) was taken from a Postfix users' mailing list.(10) First, the filter checks whether mail contains the "W32/Sircam" phrase "Hi! How are you!=3F." Then, the filter checks whether the mail attachment has a double file extension, such as "vbs.pif.," enabling it to reject "W32/Sircam" and its variants. As described, the filter should be able to detect specific expressions allowing it to be applied to other malicious mail. We used the "W32/Nimda" phrase to test this.

RESULTS

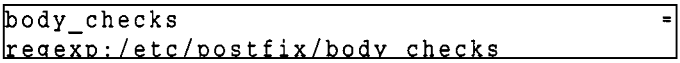
The system log (List 3) shows that the MTA rejected "W32/Sircam" and transferred other mail normally. We adopted the filter 1 day after we had received the first mail contaminated with "W32/Sircam," and the next day, this filter successfully rejected all "W32/Sircam" mail without delaying mail transactions, thereby ending the "W32/Sircam" epidemic (Fig. 2) on our network.

DISCUSSION

From the beginning, the Internet has been constructed and managed by well-intentioned people, using an open network policy and protocols. It has expanded and grown worldwide into a standard global network. There are many helpful medical applications on the Internet.(2–5)

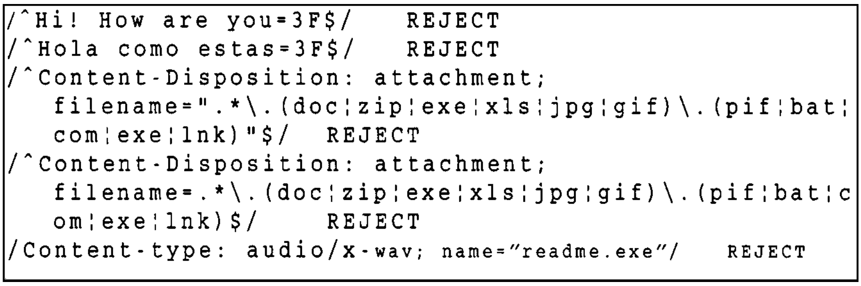
Some malicious individuals seek to attack the vulnerability of the Internet; CERT® has reported a rapid increase in such incidents.(6) Health information systems usually adopt Internet security measures, including restricted access policies, multilevel firewalls, and verbose encryption for site-to-site data transmission.(6,7)

List 1. The main.cf (Postfix configuration file) included the following phrase to enable the filter.



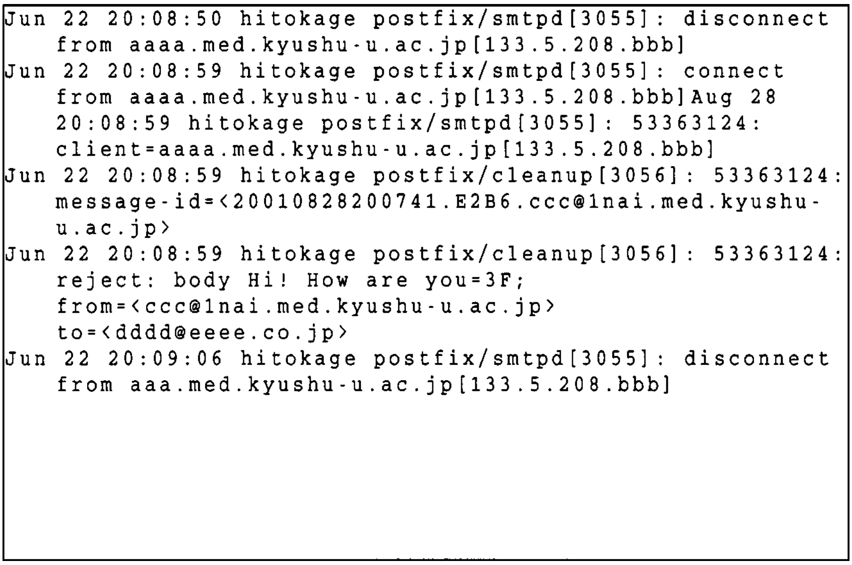
```
body_checks                                                    =
regexp:/etc/postfix/body_checks
```

List 2. body_checks. The body of the filter checks for "W32/Sircam" phrases and extensions using PCRE (Perl Compatible Regular Expression) obtained from a Postfix users' mailing list (http://www.postfix.org/lists/). Lines 1 and 2 check for the "W32/Sircam" phrase. Lines 3 and 4 check for the "W32/Sircam" attachment files. Line 5 checks for the "W32/Nimda" phrase.



```
/^Hi! How are you=3F$/    REJECT
/^Hola como estas=3F$/    REJECT
/^Content-Disposition: attachment;
   filename=".*\.(doc|zip|exe|xls|jpg|gif)\.(pif|bat|
   com|exe|lnk)"$/  REJECT
/^Content-Disposition: attachment;
   filename=.*\.(doc|zip|exe|xls|jpg|gif)\.(pif|bat|c
   om|exe|lnk)$/    REJECT
/Content-type: audio/x-wav; name="readme.exe"/    REJECT
```

List 3. This log shows that our mail server, "hitokage," checked the mail and rejected contaminated mail. The e-mail address, IP address, and host name are hidden for privacy.



```
Jun 22 20:08:50 hitokage postfix/smtpd[3055]: disconnect
   from aaaa.med.kyushu-u.ac.jp[133.5.208.bbb]
Jun 22 20:08:59 hitokage postfix/smtpd[3055]: connect
   from aaaa.med.kyushu-u.ac.jp[133.5.208.bbb]Aug 28
   20:08:59 hitokage postfix/smtpd[3055]: 53363124:
   client=aaaa.med.kyushu-u.ac.jp[133.5.208.bbb]
Jun 22 20:08:59 hitokage postfix/cleanup[3056]: 53363124:
   message-id=<20010828200741.E2B6.ccc@1nai.med.kyushu-
   u.ac.jp>
Jun 22 20:08:59 hitokage postfix/cleanup[3056]: 53363124:
   reject: body Hi! How are you=3F;
   from=<ccc@1nai.med.kyushu-u.ac.jp>
   to=<dddd@eeee.co.jp>
Jun 22 20:09:06 hitokage postfix/smtpd[3055]: disconnect
   from aaa.med.kyushu-u.ac.jp[133.5.208.bbb]
```

Because the novel and malicious code of "W32/Sircam" has the potential to leak confidential clinical patient records, and cannot be easily monitored, we used a filter on the MTA. If we adopted more restrictive checking rules, the MTA might reject normal mail and intrude on the privacy of users. Every user is informed of mail

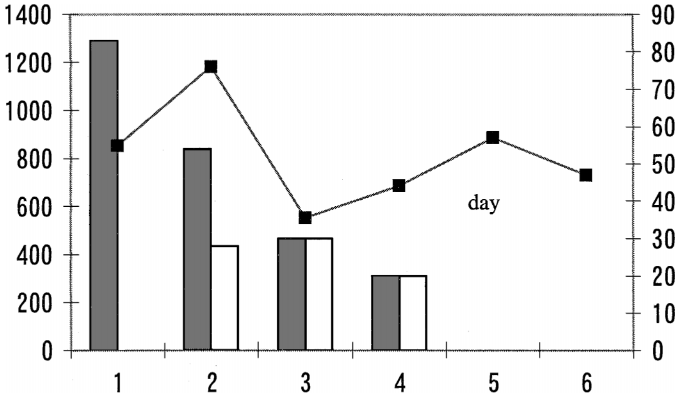


Fig. 2. "W32/Sircam" epidemic. "W32/Sircam" reached our mail server on Day 1 and we adopted the filter the next day. The epidemic ended after 4 days. The line shows the total mail the server transferred (on the left axis). The solid bar is the number of contaminated e-mails and the open bar shows the number of e-mails the filter checked and rejected (on the right axis).

security policy, but some people do not check any of their mail carefully, so ultimately the mail filter must be used on each computer and operating system.

It is very significant that a firewall, site-to-site security model does not guarantee protection against "W32/Sircam," so we must develop the next generation of security model.

REFERENCES

1. Wheeler, D. L., Church, D. M., Lash, A. E., Leipe, D. D., Madden, T. L., Pontius J. U., Schuler, G. D., Schriml, L. M., Tatusova, T. A., Wagner, L., and Rapp, B. A., Database resources of the National Center for Biotechnology Information. *Nucleic Acids Res.* 28(1):10–14, 2000.
2. Aris, I. B., Wagie, A. A., Mariun, N. B., and Jammal, A. B., An Internet-based blood pressure monitoring system for patients. *J. Telemed. Telecare* 7(1):51–53, 2001.
3. Danier, P., Le Beux, P., Delamarre, D., Fresnel, A., Cleret, M., Courtin, C., Seka, L. P., Pouliquen, B., Cleran, L., Riou, C., Burgun, A., Jarno, P., Leduff, F., Lesaux, H., and Duvauferrier, R., A network of web multimedia medical information servers for a medical school and university hospital. *Int. J. Med. Inf.* 46(1):41–51, 1997.
4. Interhospital network system using the world wide web and the common gateway interface, *J. Digit. Imaging* 12(2 Suppl. 1):205–207, 1999.
5. CERT® Coordination Center, CERT/CC Statistics 1988–2001 Number of incidents, 2001. Available from: http://www.cert.org/stats/
6. Bergeron, B., Is it safe? Security speed bumps on the information highway. *J. Med. Pract. Manage.* 16(6):297–300, 2001.
7. Sakamoto, N., A secure framework on the basis of public key infrastructure for dynamic healthcare information services in wide area distributed environments, *Japan J. Med. Inf.* 20(2):125–134, 2001.
8. Danyliw, R., Dougherty, C., and Householder, A., CERT® Advisory CA-2001-22 W32/Sircam Malicious Code, 2001. Available from: http://www.cert.org/advisories/CA-2001-22.html
9. Danyliw, R., Dougherty, C., Householder, A., and Ruefle, R., CERT® Advisory CA-2001-26 W32/Nimda Worm, 2001. Available from: http://www.cert.org/advisories/CA-2001-26.html
10. Postfix users mailing list, http://www.postfix.org/lists/