4

Raging Computer Viruses

TETSUYA YAMAZAKI
Information and communications Research Unit

4.1 Introduction

Around July and August 2001, two types of viruses*1—SirCam and CodeRed/CodeRed II—were running rampant. Developed for malicious purposes, both are highly infectious and capable of generating severe symptoms (damage from infection).

Malicious programs such as viruses, worms, and Trojan horses*1 are causing increasingly serious damage as they become more sophisticated year after year and as they spread more quickly via the highly prevalent Internet.

This report summarizes recent trends in computer viruses, with emphasis on the above two viruses.

4.2 Virus overview

4.2.1 SirCam

(1) Characteristics

SirCam, a virus/worm that made its first appearance on July 17, 2001, is distributed via e-mail attachments. When a recipient opens an infectious attachment, the virus program is loaded onto the PC to start the following activities.

SirCam sends e-mails to e-mail addresses registered in the address book of MS Outlook/Outlook Express and in files included in the Internet Temporary Files folder of the infected system. Each message has an attachment that contains a document or an image file randomly selected from the PC's My Document folder as well as a copy of the virus program. The title of each message is equivalent to the one for the file selected as its attachment, while the body is written in English or Spanish. The messages are transmitted by the worm itself without leaving any records on the e-mail software, so that the user often does not notice it.

In addition, this virus does the following damage.

1) There is a certain chance that SirCam may delete all files on the C drive on October 16.
2) There is a certain chance that SirCam may fill up the vacant hard disk space at startup of PC.

Due to a bug in the program, SirCam does not work on Windows NT/2000. In addition to this, anti-virus measures, such as removing viruses at the server level, which major businesses and some ISPs have taken in response to past virus threats, prevented this worm from being as widespread as Love Letter (also known as "I love you"), a malicious program discovered in May 2000. Yet SirCam seems rampant among private users. The Information-technology Promotion Agency, Japan (IPA), the nation's virus watchdog organization, received a total of 1,441 reports (22% of them about actual infection) on SirCam from July 21 through August 20, 2001. In particular, in August, the number of filed reports hit a record high (1,257 reports) for a single virus within a month.

(2) Actual damage

By sending a randomly selected file as e-mail, SirCam exposes personal or corporate information to a third party. In fact, official documents of the FBI and the Ukrainian government have leaked out as a result of the virus. In Japan, computers at the prefectural governments of Nagano and Shiga were infected. According to an estimation by Computer Economics, Inc., an American IT research company, more than 2.3 million computers throughout the world will have become infected with SirCam by the end of August 2001, making individuals and enterprises lose as much as a total of $1 billion as the cost for disinfection, lost productivity, and so on.

4.2.2 CodeRed/CodeRed II

(1) Characteristics

Targeting Microsoft Windows NT/2000 machines, CodeRed is a worm that attacks computers by exploiting a security hole in the Web server program known as IIS (Internet Information Server). A security hole is a vulnerability that causes security problems such as having the security check function deactivated by certain operations.

Having emerged on July 13, 2001, the worm was particularly running rampant on July 19 as it infected an estimated 250,000 plus machines worldwide in 9 hours. Microsoft estimates that 6 million computers throughout the world have the risk of infection.

After entering a computer, CodeRed carries out the following operations.

- After two hours from the time of infection, the infected system starts to display a message,"Welcome to http://www.worm.com! Hacked by Chinese!", whenever the client PC accesses a Web page through the infected server, and this symptom lasts for eight hours.
- From the 1st to 19th every month, the virus carries out infectious attacks on computers with IP addresses it randomly generates.
- From the 20th to 27th every month, all infected servers launch a DDoS*2 attack against the White House's Web site.
- From the 28th to the last day of every month, the virus stops operation to pause.

The White House has changed its Web site address at July 19 to avoid DDoS attacks by CodeRed.

CodeRed became active again on August 1, and caused further damage. CodeRed Ver. 2, a variant of CodeRed, was discovered on July 19, followed by the more destructive version CodeRed II, found on August 4.

Instead of defacing Web pages, CodeRed II creates a backdoor (a secret entrance for hackers) on the infected server so that the hacker can take control of the server. In addition, as CodeRed II generates a wider range of IP addresses to define targets for attacks, infection may become more widespread.

CodeRed can also infect a private PC, as long as it has IIS installed. Even without infection, an attack by CodeRed can cause secondary damage such as network overloading and malfunction of routers and modems.

(2) Actual damage

As mentioned above, the White House's Web site was forced to change its address. CodeRed also did a lot of harm to many other Web sites including that of Federal Express in the U.S. and Hotmail, a free e-mail service provided by Microsoft, which either shut down the site or suffered interference with business due to overwhelming network traffic. In August 2001, infection spread to South Korea and China. In Japan, Tokyo Metallic Communications Corp. suffered a communication failure on their network presumably caused by this worm. IPA estimates several thousand systems nationwide have been infected with CodeRed as of August 6, 2001. Computer Economics projects that more than a million computers will be infected with CodeRed and its variants by the end of August, producing $2.6 billion worth of losses.

4.3 Trends in recent viruses

These two viruses, SirCam and CodeRed, have the typical characteristics of recent malicious programs.

File viruses such as SirCam are typically passed with files via e-mail, and start working only when the recipients open the files. However, SirCam uses a technique to transmit infectious e-mail by itself to dramatically increase its infection route.

SirCam also uses psychological tricks such as making believe the infectious e-mail is from a friend by using the address book of the infected PC and adding a random title to the infectious message and its attachment for disguise. Similar types of viruses including Love Letter are increasing these days.

On the other hand, a new type of virus has been discovered, that can be embedded in an e-mail message body to infect the e-mail recipient's computer even if no attachment is opened (VBS. Happy Time, etc.). Also found (on August 18, 2001, in Japan) was not a virus but a kind of malicious program that can infect and crash a system when someone just accesses certain Web pages. Aside from the trend toward greater speed of infection, an increase of viruses that are passed through instant messaging (IM) services and mobile information devices, which have recently prevailed, is posing a new threat.

CodeRed is a virus designed to change Web pages without authorization and carry out DDoS attacks. This kind of virus is often used for political demonstrations, as in the case of the attack against the White House's Web site. Another obvious trend is the growth of viruses that, just like CodeRed II, intend to steal information by creating a hacking program on the infected computer. These new characteristics, which are not seen in conventional-type viruses, indicate a change in the nature of virus writers.

4.4 Developments in virus protection

A SirCam virus is loaded onto a system only when the virus program attached to an e-mail is opened. In addition, anti-virus software developers updated their virus pattern files*3 to prevent SirCam immediately after it was discovered. If uses had been more cautious, the virus would have been less rampant. On the other hand, when the security hole that CodeRed exploited for infection had been found on June 19, 2001, a patch (an additional program to fix bugs) to repair it was published by Microsoft together with an alert about the risk of a hacker making ill use of the vulnerability to take over servers. The security threat was obvious since, in early July, a program that can make an unauthorized entry into servers through the security hole was distributed online (it was removed afterwards). If every vulnerable computer had applied the patch, there would not have been any problems.

In practice, however, either of these viruses spread so widely that a great deal of harm was done. Here are possible reasons.

Many computer users, especially home users, are not well aware of the risk of viruses and the need for updating their virus pattern files.

Many companies do not understand how critical security measures are and thus do not take complete security measures. SOHO businesses, in particular, often do not even have a dedicated system administrator with sufficient skills.

System administrators are not able to keep their systems up to date and secured, since security vulnerability alerts are being issued on a weekly basis. For example, as only to the security information related to IIS, Microsoft posted as many as 25 notices on its Web page over the past one year.

While security information is released at an early stage on the Internet, other major media usually do not report it until damage becomes widely known. For example, SirCam made its first appearance in a major newspaper, the evening edition of Mainichi Daily News, on July 24, 2001, and CodeRed was first reported in Asahi Shimbun's evening paper on July 31.

Even though an increasing number of malicious program writers have been captured recently, the authorities have yet to catch up with the growth of viruses. As creating viruses is becoming easier with a variety of tools available on the Internet, complete eradication of all viruses is virtually impossible.

In addition to traditional security services for enterprises, a new service to provide mail- virus detection on ISP servers has recently been introduced as an effective means to prevent viruses. In Japan, NDS, an Okayama-based ISP company, started this service in July 2001, followed by the leading ISP Nifty in August. Meanwhile, Symantec, an anti-virus software developer, and IBM jointly developed a technology called "Digital Immune System." The system, in response to primary infection of a new virus, immediately updates the virus pattern file and anti-virus program to be distributed to every subscriber to the service. While another ongoing approach is to develop a technology to detect a new virus without its virus definition, it will take much more time to bring into actual use.

Considering that more and more computers are expected to be used in households through the widespread use of broadband connectivity and with networked home appliances, individual-level protection is critical to reduce damage attributed to viruses. To this end, further efforts to promote basic virus protection as well as to enhance fundamental anti-virus education through facilities that provide education on IT is asked for. Also important is earlier public attention to at least highly destructive viruses via popular media such as TV and newspapers.

*Online news sites including ZDNN and Nikkei Biz, and Web sites of the Information-technology Security Center at IPA, anti-virus software developers, Computer Emergency Response Team (CERT) at Carnegie Melon University, the National Infrastructure Protection Center (NIPC) in the U.S., and so on, were referred to during the research for this report.

Explanation of terms

*1 viruses, worms, and Trojan horses

A program that does harm to a computer is generally called a virus. When narrowly defined, a virus is a program that; (1) resides in another file and becomes active when it is opened, (2) creates a copy of itself in other files or computers upon infection, and (3) shows symptoms after a certain incubation period or at a preset trigger.

Worms are different from viruses in that; (1) they are independent and do not need host files, and (2) they are enabled to search for and infect targets by themselves.

A Trojan horse, while looking like an innocuous program, carries out in the background operations that the user of the infected system does not intend.This malicious program is different from viruses and worms in that it is not always infectious. However, many of the recent malicious programs combine the characteristics of the above three, just like SirCam, which is classified as a worm as well as a Trojan horse by some organizations.

*2 DDoS (Distributed Denial of Service) attacks

In a DoS (Denial of Service) attack, a targeted Web site or network is swamped with an overwhelming amount of simultaneous accesses, so that the service it provides grinds to a halt. For a DDoS attack, a type of DoS attacks, the attacker typically takes control of a large number of third-party systems through hacking or other techniques to launch DoS attacks from multiple places.

*3 virus pattern file

This file contains a database of patterns that are specific to virus programs. Anti-virus software uses these patterns to detect viruses. As the pattern varies by virus, users are required to keep their virus pattern files up to date in order to prevent new viruses.