Examples of Problems with Viruses and Unauthorized Access

Abstract

NTT East Technical Assistance and Support Center is consulted daily about various technical problems, and IP (Internet protocol) service has recently been a frequent topic. A detailed investigation has shown that most of these problems are caused by computer viruses and unauthorized access. This article describes some of the problems and explains the need for countermeasures against such threats on the Internet.

1. Broad popularity of the Internet

ADSL (asymmetric digital subscriber line), optical access, and other such always-on broadband services are now widely available to households at moderate cost, and we are entering an era in which the Internet is intimately involved in our daily lives. This situation brings with it a wider range of exposure to threats from the Internet. While computer viruses, unauthorized access, and other such harmful phenomena clearly occur, the problems may continue unresolved because the victims may be unaware of the effects.

2. Internet threats

The results of monitoring malicious incoming packets from the Internet over an arbitrary one-day time period are plotted against TCP (transmission control protocol) port number in **Fig. 1**. Except for processes certified by the Internet service provider (ISP), there were no out-going packets at all. Immediately after the computer system was connected to the Internet and obtained a global IP (Internet protocol) address, however, TCP packets that attempted to invade it were observed. Most of the attempts targeted TCP ports 135 and 445, which are frequently used for communication by the Windows operating system and are known targets for computer viruses and unauthorized access. Although the observation ended after 24 hours, we know that the attacks continued afterwards without cessation. The same results were obtained even after the global IP address was changed. These findings show that routers and personal computers that are directly connected to the Internet are constantly under attack.

† NTT East
Shinagawa-ku, 141-0022 Japan
Contact: gikyo@ml.east.ntt.co.jp

3. Examples of problems

Here, we introduce two specific examples of problems. In both of these cases, we were consulted about phenomena with unknown causes for which troubleshooting had been done locally.

(1) Unknown dial-up connection charges

This example involves connection to a measured-charge ISP via an INS64 line by means of the router's automatic connection function, as shown in **Fig. 2**. When there are Internet communication packets from a personal computer served by the router, the router's automatic connection function executes automatic authentication and connection; when there are no communication packets, it executes automatic disconnection (no-communication monitoring timer). The customer reported not using the Internet for long periods of time, so the bill was thought to be incorrect.

Investigation revealed that the connection to the Internet was continuous over a long time. Packet monitoring conducted in a more detailed investigation showed that there was no automatic disconnection after the customer had stopped using the connection, and two kinds of special packets continued to be sent from the Internet. One kind was ICMP (Internet control message protocol) packets to which the router had been responding. The other kind was surmised to

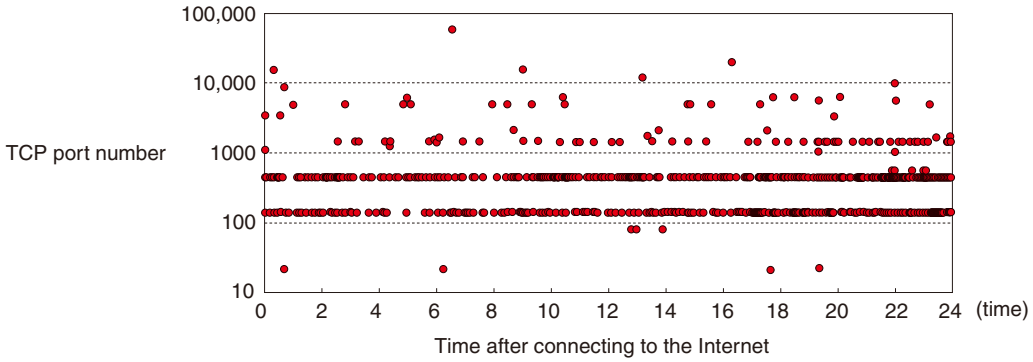

Fig 1. Observed malicious TCP packets.

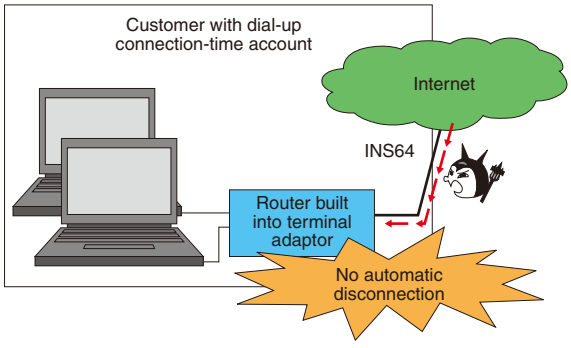

Fig 2. Hardware configuration for the dial-up connection charges example.

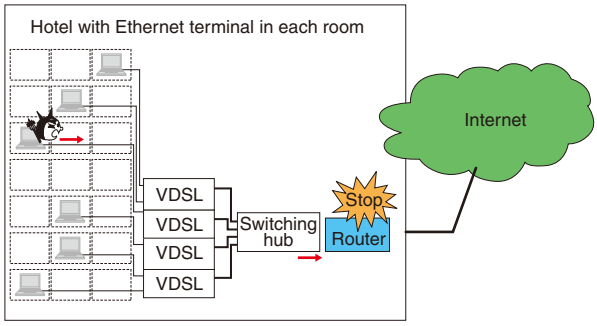

Fig 3. Configuration of the Internet hotel facilities.

be packets of the MS-Blaster computer virus attacking TCP port 135. Because packets of these kinds, and ICMP packets in particular, were being sent, the no-communication monitoring timer did not activate, even after the customer had finished using the Internet, and the connection continued without the customer being aware of it.

(2) Internet hotel router stoppage

The second example involved the frequent stoppage of the router in a long-stay hotel that has an Ethernet terminal in each room, as shown in **Fig. 3**. Each room is connected to the router with a VDSL (very high-bit-rate digital subscriber line), and the router is connected to the Internet via an always-on optical access service. Conductive noise around the router was investigated as the suspected cause of the server going down, but no particular noise was detected. The temperature around the router was also suspected, but measurements revealed no abnormal temperature environment. Then, the uplink and downlink communication data of the router was monitored and analyzed. This revealed that the personal computer in one particular room had been sending a large volume of packets to the Internet. That computer was infected with a virus that was creating such a high volume of packets that the router could not process them.

4. Countermeasures

For commercial networks and well-known Web sites, a secure firewall can be set up, but for ordinary houses and condominiums, the reality is that countermeasures that involve fees are difficult to implement. It is essential to first implement the following three measures, which do not involve charges.

(1) Use anti-virus software (with the most recent pattern files) for personal computers.

(2) Update the personal computer operating system and router firmware to the most recent version, if possible.

(3) Avoid changing computer or router security settings carelessly.

The problem in the first example can be countered by using router firmware and security settings with measures (2) and (3) above. The second example

problem cannot be dealt with easily by (1), but updating the router firmware (2) is effective.

5. Conclusion

The interface by which personal computers and routers connect to the Internet can be accessed from anywhere in the world with little effort. Computer virus attacks and attempts at unauthorized access are constant threats. To enable customers to use the Internet in the most comfortable way possible, we must reassess Internet threats and prevent problems before they occur.