Expert Insights

Recent Cyber-attacks and How Organizations Can Respond

Ryoichi Sasaki

Professor
Department of Information Systems and Multimedia Design
Tokyo Denki University

Graduated from The University of Tokyo and entered Hitachi, Ltd. in 1971 where he worked at the Systems Development Laboratory on topics that included techniques for improving system reliability and security technology. He took up his current post in April 2001.
Doctor of Engineering (University of Tokyo); Chairman, Japan Society of Security Management; Advisor on Information Security, National Information Security Center; Visiting Professor, National Institute of Informatics.
His publications include "Introduction to Internet Security" (Iwanami Shinsho, 1999) and "Concept of IT Risk" (Iwanami Shinsho, 2008), both in Japanese.

Along with attacks from hackers motivated as much as anything by their own amusement, the increasing diversity of cyber-threats also encompasses a growing number of sophisticated attacks from spies and the like seeking to obtain confidential information. A well-known form of this latter threat is the following type of targeted e-mail attack.

Step 1: Initial intrusion: An e-mail with a virus-infected file attachment is sent to the personal computer (PC) of a key person at the targeted organization. Opening the file causes the PC to become infected.

Step 2: Escalation of intrusion: An attempt is made to penetrate servers on the local network from the infected PC.

Step 3: Mission accomplished: Confidential information is stolen from the infected PC or servers.

A targeted e-mail attack differs from a conventional spam attack in various ways. These include, (1) The content of the e-mail is chosen specifically for the individual targeted so as to encourage them to open the file, (2) The small number of such attacks means that the anti-virus provider may not be aware of the virus's existence, and therefore virus scanning may be unable to detect and remove it, and (3) Once a PC is infected, it can make ongoing attempts to access servers on the local area network (LAN) with the aim of acquiring information.

Just because you believe that no spy would have reason to mount a targeted e-mail attack on your own company is no cause for complacency. It is not unknown for such attacks to start, not by attacking the target directly, but by stealing information from affiliated companies or customers that can then be used to penetrate the real target company.

A growing trend in recent times has been the use of "water hole attacks" that attempt to infect computers with a virus by illicitly tampering with websites frequented by users at the targeted organization. To make it difficult to detect which websites have been compromised, a common practice is to only attempt infection in response to access from specific Internet protocol (IP) addresses, such as those of government agencies.

As we approach the Tokyo Olympics in 2020, we can expect cyber-attacks on Japan to become increasingly sophisticated and diverse. Equipping our organizations with the capabilities to put comprehensive countermeasures in place is a matter of urgency.