Keywords A to Z Vol.12

Keyword Malware

A collective name for malicious software that sneaks into users' computers through, for example, e-mail attachments, and exhibits malicious behavior such as stealing private/confidential information, destroying and manipulating data, etc.

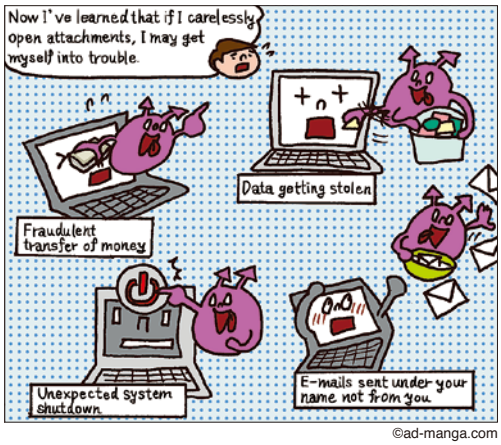
Malicious behavior by malware threatening computer users

Today we live in a world that will not work without information technology and computer networks. While at the same time, the threat by malware continues to increase. Malware is a coined word made up of mal as in malicious and ware as in software. Malware sneaks into devices, such as PCs and smartphones, to take malicious actions, such as stealing private/confidential data, destroying and manipulating such data, etc.

Generally, malicious software program spreads from computer to computer via a network such as the Internet by infecting many and unspecified users' computers through infected e-mail attachments and infected files supplied by external devices. That is why it is also called computer virus. In around the 2000s, for instance, a devastating computer virus called LOVELETTER spread across the globe. This virus was sent via e-mail messages with the subject line "I Love You," and when the e-mail recipient opens the attachment, that attachment or file is activated to send a copy of itself to all addresses in the mailing software installed on that recipient's computer. This virus, however, was more like a crime of pleasure, considering less threatening than that of today's malware in terms of criminal intent.

In recent years, however, there have appeared new types of malicious software programmed to attack a specific organization to wreak havoc, which is threatening to many companies, countries, and autonomous bodies. This is a kind with a clear criminal intent acting in various unexpected ways like stealing and manipulating and/or leaking confidential information. These viruses are collectively called malware.

Malware is a threat not only for organizations but also for many individual computer users. A virus attack known as ransomware is one of the malware families whose threat has rapidly risen in recent years. Like other malware families, ransomware reaches a victim's computer in form of an e-mail attachment and installs covertly on the computer and encrypts certain file types on the infected system so the victim cannot access them. Then the attacker sends an e-mail to the victim and asks for a ransom in exchange of decrypting the victim's locked files.



©ad-manga.com

Countermeasures against the threat by malware that is lurking in today's convenience

Generally, organizations like companies implement a multi-layered defense system, installing anti-virus software on their computers and servers, and at the same time they also install defense programs such as Firewall and Firewall devices to establish barriers between the company's intranet and outside networks. They also implement strong measures in their operations by making rules that stipulate strange e-mails and files should never be opened and have their employees follow these rules.

In spite of these efforts, there is no end to the attacks by viruses targeting a specific organization. If a virus invading a specific organization is specially programmed for that organization, there cannot be a match between existing virus definitions and this invading virus, and thus anti-virus program cannot detect it. In addition, malware is sent dexterously outwitting the company's rules, pretending the e-mail is from the recipient's boss, peer, or acquaintance so that the recipient lets his guard down and opens it.

Accordingly, there is no perfect way to prevent malware invasion. Therefore, in addition to the existing active scanning (detection before infection) method, some people emphasizes the importance of passive scanning (detection after infection) to capture the behavior of malware after it gets into the system.

So, what can we as individuals do to protect our computers from malware? Like many organizations, we need to install anti-virus software in our PCs and smartphones and update these applications constantly. We also need to be careful not to open suspicious attachments. When accessing some website for the first time, we should think about their security, whether we can trust them or not, because visiting websites is one of the major causes.

IT and computer networks have made our world an extremely convenient place. But this convenience and the threat by malware are two sides of the same coin. We always have to be aware of the threat and should make constant efforts to gather information about malware, save confidential data on external hard drives instead of on our computer's hard drives, and mix various ways of communication, such as telephones and fax machines, instead of relying on the e-mail exchange alone. Computer users need to take actions infallibly to create a safe environment to use their computers.

Cover photo by Koji Mizutani, MERRY PROJECT Representative

azbil
http://www.azbil.com/
Yamatake Corporation changed its name to Azbil Corporation on April 1, 2012.

azbil Group PR magazine, azbil 2017 Vol. 2, No. 7
Issued by Mikako Takahashi, Public Relations Section, Corporate Planning Department, Azbil Corporation
19F Tokyo Building, 2-7-3 Marunouchi, Chiyoda-ku, Tokyo 100-6419 Japan TEL: 81-3-6810-1006 FAX: 81-3-5220-7274
URL: http://www.azbil.com/

PRINTED WITH SOY INK
MIX Paper from responsible sources FSC® C002215

PR-3001E-1704 (1704-4K-D)

Company/Branch office