MUCH ADO ABOUT MALWARE

By Zahri Yunos and Sharmila Mohamad Salleh

(This article was published in NST Tech & U on 4 June 2007)

AS connectivity continues to improve, malicious programs or Malware have become more and more prevalent. Malware is dangerous because they can interfere with the computer's ability to process information, and modify or destroy important data. Malware frequently comes in the form of mass-mailing worms that infects computers - usually, after an unwitting user has opened an attachment such as via e-mail, containing the worm.

Malware also tends to propagate itself via other e-mail addresses found on the infected computer. Statistics compiled by MyCERT (www.mycert.org.my) showed 61 reported incidents involving malware last year up to the month of October. Of these, 44 incidents involved worms (self-replicating malicious programs), 12 incidents involved Trojans (a seemingly safe program that contains malicious code) and five incidents involved Bots (automated malicious programs that react to pre-defined events). Internationally, some of the more famous malware incidents of 2006 included:

TROJANS THAT DEMAND RANSOM. Security Focus (www.securityfocus.com) reported that the malicious program infects a computer, encrypts a user's data and threatens it with deletion, blackmails the computer users and then demands a ransom should the user want the data back. Similarly, Security Pipeline (www.securitypipeline.com) on March 16, 2006 reported Trojans that lock up files and then demand money as ransom to return access. Dubbed Cryzip or Zippo.a, the Trojans archives several file types, including .doc (Microsoft Word), .pdf (Adobe Acrobat), and .jpg (images), within a ZIP library, then password-protects the files and deletes the originals. A ransom note is left on the machine demanding a US$300 ransom.

TROJANS THAT ATTACK GOVERNMENT NETWORKS. The United States Department of Homeland Security on June 21, 2006 reported that several political groups in the US have begun a systematic assault of governmental and other political groups' computer systems and networks. The method goes like this: a thumb drive is left lying in an obvious place. The idea is that an employee of the targeted agency will pick up the thumb drive and try to identify who the device belongs to by inserting it into a computer inside the building. The thumb drive contains files that are given titles that entice the finder of the device to open it. Once the file is opened, Trojans will be uploaded to the computer and attack the computer and any networks it is connected to. In another case, the Government of India was put on a high alert after a Trojan was detected in the computer networks of various Government Departments of India. The Itb Virus (www.itbvirus.com) on Dec 27, 2006 reported that the Trojan is spreading among targeted networks with the help of an e-mail attachment named as Cabnote, which pretends to be a document from the cabinet or the ministry and thus tricking recipients to open it.

TROJANS THAT SPOOF EMAILS FROM ANTI-CHILD PORN AGENCY. Sophos (www.sophos.com) on August 22, 2006 has warned of a Trojan that was distributed via an e-mail claiming to come from an organisation fighting child pornography on the Web. The e-mails claim that the recipient's e-mail address has been found on a child porn database discovered by the Association of Sites Advocating Child Protection, but what it really contains is a Trojan horse.

VIRUS THAT COMPROMISES CONFIDENTIAL FILES. The Register (www.theregister.co.uk) on May 17, 2006 reported that sensitive information about Japanese power plants has leaked online from a virus-infected computer for the second time in four months. The first incident occurred in January 2006. Data regarding security arrangements at a thermo-electric power plant run by the Chubu Electric Power in central Japan spilled online as a result of an unnamed virus infection. The name and addresses of security workers, along with other sensitive data including the location of key facilities and operation procedures were leaked to the public. It is suspected that a subcontractor at the plant who installed a file- sharing program on his PC was the source of the incident.

WORLD CUP WORMS. Not content with letting people enjoy the once in four years spectacle, SC Magazine (www.scmagazine.com) on June 21, 2006 reported two new e-mail worms which exploited interest in the World Cup, attacking computers and turning them into part of a Botnet. The Sixem-A and W32.Worm.Zade.A worms spread using a variety of disguises such as tricking computer users into clicking on a malicious attachment. In another example, eWeek (www.eweek.com) on May 8, 2006 reported that a new virus infects Microsoft Excel files. Identified as XF97/Yagnuul-A, the virus lives in an Excel file that offers to help people set up fantasy sports competitions related to the international soccer championship, and attempts to market itself specifically to fans of the English Premiership. Once the virus infected a user's computer, it begins forwarding itself to other people using the corrupted machine and sends itself to people listed in any e-mail client software on the device.

PROTECTION TIPS. The following tips, while not total solutions, go a long way towards protecting PCs from malicious programs.

1) Install anti-virus software and personal firewall software. For Windows-based PC users, free-for-noncommercial-use software such as AVG (www.grisoft.com) and Zone Alarm (www.zonelabs.com) protect your computers against malicious program such as viruses, Trojans and all sorts of malware. Make sure to keep your definitions up to date.

2) Regularly install operating system and application software patches so that known problems or vulnerabilities can be updated. For Windows PC users, the site to visit is www.windowsupdate.com.

3) Avoid the use of unlicensed software programs. It is advisable to use legitimate software programs only. One of the ways malware is distributed is through compromised unlicensed software distributions.

4) Do not randomly allow other people to use your computer. They may accidentally infect your computers with viruses or Trojans that modify and/or delete your files.

5) Follow corporate policies for handling and storing work-related information. Ensure your data is backed up regularly.

6) Follow good security habits. You may want to review other security tips for ways to protect your data from being infected by malicious programs.