BEWARE THE HIDDEN DANGER

By

Ahmad Nasir Mohd Zin and Zahri Yunos

National ICT Security and Emergency Response Centre (NISER)

(This article was published in The Star InTech on 28 Feb 2006)

Introduction

Incidents of espionage as a way of getting military, political or economic secrets have been well documented throughout history, while the method of using a "Trojan" (the Trojan horse) to penetrate the enemy defensive position is a well known exploit in Greek mythology, known as the Trojan war.

The end of the Cold War has resulted the espionage activities been diverted to industrial espionage. Industry players seek competitive advantage by obtaining or stealing its competitor's trade secrets and logistics. The attacks are highly targeted to gain the specific information sought. Companies will devote the necessary resources towards industrial espionage to achieve an acceptable return on investment.

Corporate espionage is a threat to any businesses whose livelihood depends on information.[1] It can also be defined as the theft of trade secrets through illegal means such as wiretaps, bribery and cyber intrusion.[2] In year 1999,

[1] Robinson, S., Corporate Espionage 101,version 1.3, SANS Institute 2003 http://www.sans.org/rr/whitepapers/engineering/512.php , last visited 10 February 2006.
[2] Business Week Online, The Case of the Corporate Spy, In recession, competitive intelligence can pay off big, 26 Nov 2001, http://www.businessweek.com/magazine/content/01_48/b3759083.htm, last visited 13 February 2006.

Price Waterhouse Coopers reported that U.S. firms lose US$45 billion to espionage, nearly twice the estimate given a few years earlier by the FBI.[3]

Recent development shows that corporate espionage using Trojan is on the rise. With rapid advancement of ICT, espionage activities have been carried out using ICT technologies. These types of cyber attacks are targeted at specific recipients to get past firewalls and gather sensitive data.

Trojan "hide malicious code" inside a host program that seems to do something useful. Once these programs are executed, the virus, worm or other types of malicious code hidden in the Trojan program is released to attack the workstation, server, or network, or to allow unauthorised access to those devices. Trojans are common tools used to create backdoors into the network for later exploitation by hackers.[4] By creating backdoors of the corporate networks, the hackers could steal corporate secrets or use the compromised computers to send spam and viruses.

Below are some cases of industrial espionage as reported in the media.

Case 1: Myfib

Myfib Trojan first appeared in August 2004. This Trojan is sent by spam and can navigate a computer network once the attachment is clicked. A US security firm, Lurhq has reversed engineered Myfib codes for clients and discovered that the Trojan was sending stolen data to an Internet user in Tianjin, China.[5] The program appears to have originally developed to steal student exam papers and later expanded to copy many types of documents such as computer assisted drawing and Microsoft Word files. It has been

[3] Sullivan, B., Israel espionage case points to new Net threat, Experts: Targeted spy attacks could be soon be common, MSNBC, 9 June 2005, http://www.msnbc.com/id/8145520/page/2, last visited 10 February 2006.
[4] Krutz, R.L., and Vines, R.D., The CISSP Prep Guide, Second Edition: Mastering the CISSP and ISSEP Exams, Wiley Publishing, Indiana, 2004.
[5] Vardi, N., Chinese Take Out, Forbes.com, 25 July 2005, http://www.forbes.com/home_asia/free_forbs/2005/0725/054.html , last visited 15 November 2005.

reported that the code has been used to steal sensitive documents such as mechanical designs and circuit board layouts.

In another case, it was reported that a group of Chinese hackers were suspected of launching intelligence-gathering attacks against the U.S government. The hackers, believed to be based in the Chinese province of Guangdong, were believed to have stolen U.S. military secrets, including aviation specifications and flight-planning software.

Case 2: Britain Attacked

In June 2005, the United Kingdom's National Infrastructure Security Coordination Centre (NISCC) provided advice and issued a briefing pertaining to targeted Trojan email attacks against the UK Government and companies.[6] NISCC believed that the principal goal of the attacks is covert gathering and transmitting of privileged information which are commercially or economically viable. These attacks used open source Trojans such as Nethief, MoFei, GWBoy, Grey Pigeon, Magic Link and Bespoke, which were being altered to avoid anti-virus detection. Once installed, the Trojan can collect usernames and passwords of email accounts, collect system information, upload documents and data to a remote computer, downloading of further programs, which can be more sophisticated Trojans, and relay further attacks against other computers and networks. NISCC discovered 17 Trojans or remote monitoring programs between April and May 2005.

Case 3: Trojan-gate

This case came to light when a husband and wife book writing team, Amnon Jackont and Varda Raziel-Jackont found out that passage from their book, which was not yet published then, was posted on the Internet. They suspected that someone has hacked into their computer system and stolen files. Police investigation traced the alleged theft to Varda Raziel-Jackont's

[6] National Infrastructure Security Co-ordination Centre (NISCC), Targeted Trojan Email Attacks, NISCC Briefing 8/2005, issued 16 June 2005, http://www.egovmonitor.com/reports/rep11599.pdf, last visited 13 February 2006.

former son-in-law, Michael Haepharati, a computer consultant. This case is dubbed the "Trojan Affair" and some are calling it "Trojan-gate". In May 2005, Michael Haepharati was detained in London together with his wife, Roth Brier-Haepharati.[7] Both were repatriated to Israel on 31 January 2006 [8], soon after the appeal court in London approved their extradition on 13 January 2005, for allegedly selling rogue computer program to Israeli private investigators who use it to spy on their clients' competitors.

The Tel Aviv Magistrate's Court has remanded several people from some of Israel's leading companies and private investigators suspected of commissioning and carrying out industrial espionage against their competitors. It has been reported that at least 18 Israeli firms have been implicated in this case.[9] The act was allegedly carried out by planting Trojan in their competitors' computers. It was discovered that Mr Haepharati had sold the rogue computer program to three private investigation agencies.

How Can You Prevent The Trojan From Installing On Your Computer?

To avoid unintentionally installing Trojans on your computer, below are some suggestions you can practice:

- Do not downloadable free software from untrustworthy source. There are many sites that offer exciting programs or software. You may be exposing your computer to Trojans by downloading some of these programs.

[7] Trojan Horse developers to be extradited to Israel soon, Hack In The Box, 18 January 2006, http://www.hackinthebox.org/print.php?sid=19044, last visited 13 February 2006.
[8] Israel holds couple in corporate espionage case, Reuters, in Yahoo! News,31 January 2006, http://news.yahoo.com/s/nm/20060131/tc_nm/crime_israel_spyware_dc, last visited 13 February 2006.
[9] 18 Arrested In Israeli Probe Of Computer Espionage, Washington Post, 31 May 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/05/30/AR2005053000486.html, last visited on 13 February 2006.

- Choose "no" when you received unexpected questions from unexpected dialog boxes. Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. By clicking the dialog boxes questions may install Trojans on your computer.

- Do not click an email attachment that is suspicious. Trojans can bypass most anti-virus software and entice the recipient to believe the e-mail transmitting the Trojans is legitimate. Instead of installing the intended document, you are actually installing Trojans.

- Run a legitimate product specifically designed to scan and remove Trojans in your computer. The Trojans probably undetectable by using normal anti-virus software and could remain hidden on the compromised computers for years.

Conclusion

Home computers and corporate networks are already bombarded by unwanted contents such as spam, phishing, viruses and worms. Perpetrators are continuously conducting in-depth research on network security and find ways on how to penetrate big corporation’s network and critical infrastructure organisations without being suspicious. The sophistication levels of attacks are increasing and it is expected that those attacks will grow more slick and secretive in the future.